#3
AM
5-18-01

Docket No.: 5899-031 **PATENT**

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of	:	
Koichi YONETA, et al.	:	
Serial No.:	:	Group Art Unit:
Filed: February 02, 2001	:	Examiner:

For: DIGITAL INFORMATION SALES METHOD

CLAIM OF PRIORITY AND
TRANSMITTAL OF CERTIFIED PRIORITY DOCUMENT

Commissioner for Patents
Washington, DC 20231

Sir:

In accordance with the provisions of 35 U.S.C. 119, Applicants hereby claim the priority of:

Japanese Patent Application No. 2000-115781,
filed April 11, 2000

cited in the Declaration of the present application. A certified copy is submitted herewith.

Respectfully submitted,

MCDERMOTT, WILL & EMERY

Michael E. Fogarty
Registration No. 36,139
Larry T. Cullen
Reg. 44,489

600 13th Street, N.W.
Washington, DC 20005-3096
(202) 756-8000 MEF:klm
Date: February 2, 2001
Facsimile: (202) 756-8087

"515" FEBRUARY 6, 2001
YONSTA etc.

McDermott, Will & Emery

日本国特許庁
PATENT OFFICE
JAPANESE GOVERNMENT

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日
Date of Application: ２０００年　４月１１日

出願番号
Application Number: 特願２０００－１１５７８１

出願人
Applicant (s): 株式会社日立製作所
株式会社日立画像情報システム

CERTIFIED COPY OF PRIORITY DOCUMENT

２０００年１２月２２日

特許庁長官
Commissioner,
Patent Office 及川耕造

出証番号　出証特２０００－３１０６２３９

【書類名】　特許願

【整理番号】　D99007291A

【提出日】　平成12年 4月11日

【あて先】　特許庁長官殿

【国際特許分類】　G06F　9/06

【発明の名称】　ディジタル情報販売方法及びディジタル情報販売装置

【請求項の数】　13

【発明者】

【住所又は居所】　神奈川県横浜市戸塚区吉田町２９２番地　株式会社日立画像情報システム内

【氏名】　米田　幸一

【発明者】

【住所又は居所】　神奈川県横浜市戸塚区吉田町２９２番地　株式会社日立画像情報システム内

【氏名】　井上　雅之

【発明者】

【住所又は居所】　神奈川県横浜市戸塚区吉田町２９２番地　株式会社日立画像情報システム内

【氏名】　名波　秀昇

【発明者】

【住所又は居所】　神奈川県横浜市戸塚区吉田町２９２番地　株式会社日立画像情報システム内

【氏名】　稲光　哲治

【発明者】

【住所又は居所】　神奈川県横浜市戸塚区吉田町２９２番地　株式会社日立画像情報システム内

【氏名】　佐藤　勝俊

【発明者】

【住所又は居所】　神奈川県横浜市戸塚区吉田町２９２番地　株式会社日立

製作所デジタルメディア開発本部内

【氏名】　伊藤　滋行

【発明者】

【住所又は居所】　神奈川県横浜市戸塚区吉田町２９２番地　株式会社日立製作所デジタルメディア開発本部内

【氏名】　高見　穣

【発明者】

【住所又は居所】　神奈川県横浜市戸塚区吉田町２９２番地　株式会社日立製作所デジタルメディア開発本部内

【氏名】　松本　健司

【発明者】

【住所又は居所】　神奈川県横浜市戸塚区吉田町２９２番地　株式会社日立製作所デジタルメディア開発本部内

【氏名】　井上　喜勇

【特許出願人】

【識別番号】　000005108

【氏名又は名称】　株式会社　日立製作所

【特許出願人】

【識別番号】　000233136

【氏名又は名称】　株式会社　日立画像情報システム

【代理人】

【識別番号】　100075096

【弁理士】

【氏名又は名称】　作田　康夫

【手数料の表示】

【予納台帳番号】　013088

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【プルーフの要否】　要

【書類名】 明細書

【発明の名称】 ディジタル情報販売方法及びディジタル情報販売装置

【特許請求の範囲】

【請求項１】

ディジタル情報を販売する方法であって、

前記ディジタル情報の利用許可を示すキー情報と、

前記キー情報が書きこまれる第１の記憶媒体から、ディジタル情報制御装置を用いて第２の記憶媒体へキー情報を複製する際に、記憶媒体所有者がアクセスできない販売者エリアへディジタル情報を利用するための料金を格納させるようにディジタル情報制御装置を制御するプログラムと、

をディジタル情報の販売の際に、第１の記憶媒体に記憶させることを特徴とするディジタル情報販売方法。

【請求項２】

ディジタル情報を販売する方法であって、

前記ディジタル情報の利用許可を示すキー情報と、

前記キー情報が書きこまれる第１の記憶媒体から、ディジタル情報制御装置を用いて第２の記憶媒体へキー情報を複製する際に、記憶媒体の記憶媒体所有者がアクセスできない販売者エリアへディジタル情報を利用するための料金を格納させる機能と、

前記記憶媒体を用いて通信を行うときに、前記販売者エリアに格納された料金を販売元へ送信するようにディジタル情報制御装置を制御する機能を有するプログラムと、

をディジタル情報の販売の際に、第１の記憶媒体に記憶させることを特徴とするディジタル情報販売方法。

【請求項３】

前記プログラムは、前記第Ｎ－１の記憶媒体（Ｎは３以上の整数）から、第Ｎの記憶媒体へ前記キー情報を複製する際にも、記憶媒体の記憶媒体所有者がアクセスできない販売者エリアへディジタル情報を利用するための料金を格納させるようにディジタル情報制御装置を制御する機能を有することを特徴とする請求項

出証特２０００－３１０６２３９

１又は２に記載のディジタル情報を販売する方法。

【請求項４】

前記プログラムは、前記第Ｎの記憶媒体の前記販売者エリアに前記利用料金を格納するように制御する機能を有することを特徴とする請求項３に記載のディジタル情報を販売する方法。

【請求項５】

前記プログラムは、前記第Ｎの記憶媒体と、前記第Ｎ－１の記憶媒体の、販売元との取り引き回数を比較し、取り引き回数の多い記憶媒体の前記販売者エリアに前記利用料金を格納するように制御する機能を有することを特徴とする請求項３に記載のディジタル情報を販売する方法。

【請求項６】

前記プログラムは、前記販売者エリアに利用購入金額を有する記憶媒体がＡＴＭ装置に挿入されたときに、前記販売者エリアに格納された金額情報をディジタル情報販売装置へ送信させるように、前記ＡＴＭを制御する機能を有することを特徴とする請求項１乃至５のいずれかに記載のディジタル情報を販売する方法。

【請求項７】

ディジタル情報を販売する方法であって、

前記ディジタル情報の利用許可を示すキー情報と、

前記キー情報が書きこまれる第１の記憶媒体から、第２の記憶媒体へキー情報をディジタル情報制御装置を用いて複製する際に、キー情報が使用不可の状態で複製されるように、該ディジタル情報制御装置を制御する機能を有するプログラムと、

をディジタル情報の販売の際に、第１の記憶媒体に記憶させることを特徴とするディジタル情報販売方法。

【請求項８】

ディジタル情報を販売する方法であって、

前記ディジタル情報の利用許可を示すキー情報と、

前記キー情報が書きこまれる第１の記憶媒体から、第２の記憶媒体へキー情報をディジタル情報制御装置を用いて複製する際に、キー情報が使用不可の状態で

複製されるように、該ディジタル情報制御装置を制御する機能と、

複製されたディジタル情報の再生する際に、前記第２の記憶媒体に記憶されたキー情報を使用可能な状態にするために、通信手段によりディジタル情報販売元にアクセスさせるようにディジタル情報制御装置を制御する機能とを有するプログラムと、

をディジタル情報の販売の際に、第１の記憶媒体に記憶させ

使用不可の状態のキー情報が記憶された第２の記憶媒体を用いてアクセスがあったときに、前記ディジタル情報の利用料金を支払いにより、前記第２の記憶媒体に記憶されたキー情報を使用可能な状態させる情報を送信することを特徴とするディジタル情報の販売方法。

【請求項９】

ディジタル情報を記憶する記憶手段と、

前記ディジタル情報の利用許可を示すキー情報を記憶する手段と、

前記ディジタル情報と前記キー情報を購入することにより前記キー情報が書きこまれた第１の記憶媒体から、第２の記憶媒体へ、前記キー情報をディジタル情報制御装置を用いて複製する際に、キー情報が使用不可の状態で複製されるように、該ディジタル情報制御装置を制御する機能を有するプログラムを格納する手段とを有し、

該ディジタル情報の販売の際に、前記キー情報と前記プログラムを購入者の記憶媒体に記憶させることを特徴とするディジタル情報販売装置。

【請求項１０】

ディジタル情報を記憶する記憶手段と、

前記ディジタル情報の利用許可を示すキー情報を記憶する手段と、

前記ディジタル情報と前記キー情報を購入することにより前記キー情報が書きこまれた第１の記憶媒体から、第２の記憶媒体へ、前記キー情報をディジタル情報制御装置を用いて複製する際に、キー情報が使用不可の状態で複製されるように、該ディジタル情報制御装置を制御する機能と、複製されたディジタル情報の再生する際に、前記第２の記憶媒体に記憶されたキー情報を使用可能な状態にするために、通信手段によりディジタル情報販売元にアクセスさせるようにディジ

タル情報制御装置を制御する機能とを有するプログラムを格納する手段とを有し、

該ディジタル情報の販売の際に、前記キー情報と前記プログラムを購入者の記憶媒体に記憶させ、

該第２の記憶媒体を用いてアクセスがあったときに、前記ディジタル情報の利用料金を支払いにより、前記第２の記憶媒体に記憶されたキー情報を使用可能な状態させる情報を送信することを特徴とするディジタル情報販売装置。

【請求項１１】

ディジタル情報の利用許可を示すキー情報が格納された第１の媒体を制御する手段と、

第１の媒体に記憶された該キー情報を第２の媒体へ複製する手段を有するディジタル情報制御装置を制御する機能を有する制御装置が読み取り可能なプログラムであって、

前記制御装置に、前記第１の媒体に記憶されたキー情報を、前記第２の媒体へ複製する際に、前記キー情報を使用不可の状態にさせ、使用不可状態のキー情報を第２の媒体に記憶させる機能を実現させることを特徴とするプログラム。

【請求項１２】

ディジタル情報の利用許可を示すキー情報が格納された第１の媒体を制御する手段と、

第１の媒体に記憶された該キー情報を第２の媒体へ複製する手段と、

複製されたキー情報が格納された第２の媒体を制御する手段と、

外部装置と通信可能な通信手段とを有するディジタル情報制御装置を制御する機能を有する制御装置が読み取り可能なプログラムであって、

前記制御装置に、

前記第１の媒体に記憶されたキー情報を、前記第２の媒体へ複製する際に、前記キー情報を使用不可の状態にさせ、使用不可状態のキー情報を第２の媒体に記憶させる機能と、

複製されたディジタル情報を再生する際に、前記第２の媒体を用いて前記通信手段により、ディジタル情報の販売装置へ通信を行わせることにより、前記第２

の媒体に記憶された使用不可状態のキー情報を使用可能な状態にする機能を実現させることを特徴とするプログラム。

【請求項１３】

前記第１の記憶媒体と第２の記憶媒体は、電子マネー情報と、ＩＣカード固有のキー情報を有するＩＣカードであり、前記キー情報が第１の記憶媒体又は第２の記憶媒体に記憶される際に、該ＩＣカード固有のキー情報により暗号化されていることを特徴とする請求項１乃至８のいずれかに記載のディジタル情報の販売方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、ディジタル情報の販売・管理システム及び装置に関する。

【０００２】

【従来の技術】

ディジタル情報の最大の特長はデータの劣化がないことである。そこで、利用者間におけるディジタル情報の不正な複製及びその利用、又はその複製したディジタル情報の販売などが深刻な問題となっている。このディジタル情報の管理する方法の一例として、特公平６－２８０３０号「ソフトウェア管理方式」（以下、ソフトウェア管理方式という）が挙げられる。

【０００３】

【発明が解決しようとする課題】

ディジタル情報の正当な利用方法の提供に際して、権利者と利用者、又は利用者間を伝達、又は複製されるディジタル情報には何らかのセキュリティ保護が必要であると考えられる。

【０００４】

上記ソフトウェア管理方式では、有償データ固有の情報を規定のメモリに記憶していることを条件に、ソフトウェアの利用を許可する。しかし、利用条件である有償データ固有の情報を各利用者の規定のメモリにコピーすれば、ソフトウェアの利用が可能となってしまう。特に、利用者間において、上記コピーが行われ

ると、そのソフトウェアはフリーソフトのごとく無償で利用されてしまう恐れがあり、権利者が受け取るべき料金が回収できなくなる危険性がある。

【０００５】

また、上記ソフトウェア管理方式では、払戻しのインセンティブにより、外部入出力処理部にて利用明細情報の報告を行うことを利用者に促すことで協会が利用明細を取得し、協会から明細の内容に合致した金額を権利者の銀行口座に振り込むことで、利用者から権利者への料金回収を実現している。しかし、通信機能を利用した利用明細の報告を行う場合、すべての利用者に通信機能が必要であるという限定がかかり、利用者に対して設備投資の負荷がかかってしまう。また、利用者間の複製ではオフライン環境下でしか稼動できないような端末での利用も考えられ、オフライン環境下の利用者への拡販が見込めないことになる。

【０００６】

【課題を解決するための手段】

そこで、本発明では、映像、音楽、著書などのディジタル情報の販売・管理を行うために、セキュリティ保護されたディジタル情報を、利用者間で利用又は複製することを可能とし、ディジタル情報の利用に伴う料金をディジタル情報の権利者へ確実に回収できる方法を提供する。

【０００７】

ディジタル情報のセキュリティ保護を行うために、ディジタル情報を再生するためのキー情報を設け、キー情報に基づき、ディジタル情報の再生を判断する。このキー情報の複製の際に、以下の２つの方法により、セキュリティの担保と料金回収を達成する。

第１の方法は、ディジタル情報とキー情報の複製の際に、ユーザーがアクセスできない販売者エリアに販売金額を格納させることとする。この方法によれば、ディジタル情報を複製したユーザーは、オフラインでディジタル情報を複製した場合あっても、キー情報が上記第１の方法と異なり使用可能であるため、ディジタル情報を利用することができる。また、販売者エリアに格納された料金を後日、オンラインや銀行ATM等により、回収することができるため、オフラインで複製した場合であっても料金を回収することができる。

【０００８】

第２の方法は、として、正規の利用者ではない他の利用者がディジタル情報を複製するときは、キー情報を使用不可の状態で複製させる。ディジタル情報の複製時には、キー情報が使用不可となっているため、キー情報をコピーしてもディジタル情報を利用できない。したがって、不正な複製による利用を阻止することができる。そして、ディジタル情報を複製した利用者は、ディジタル情報を利用する際に、販売元へアクセスして料金を支払い、使用不可のキー情報のロックを解除する。ディジタル情報の利用に際して、必ず販売元へアクセスするので、このときに料金を確実に回収することができる。

【０００９】

なお、複製の際や回収の際にこのような制御を行わせるためのプログラムを、ディジタル情報、キー情報と共に、利用者の記憶媒体に記憶させて、ディジタル情報を販売することとする。

【００１０】

【発明の実施の形態】

本発明の第１の実施例を、図１から図４を用いて説明する。第１の実施例は、ディジタル情報の利用に際してキー情報が必要であり、ディジタル情報とキー情報の複製の際に、ユーザーがアクセスできない販売者エリアに販売金額を格納させるものである。

【００１１】

図１に、本発明が適用される有料ディジタル情報の購入、転売及びその料金回収方法に関するシステムの一実施例の構成図を示す。図２に、本システムにおける著作権権利者とディジタル情報を購入する第一利用者間のディジタル情報販売手順を示す。図３に、第一利用者が購入したディジタル情報を利用するための手順を示す。図４に、第一利用者と著作権権利者から直接ディジタル情報の購入をしていない第二利用者間の複写手順を示す。

【００１２】

図１において、ディジタル情報販売装置１はディジタル情報を販売する著作権権利者や販売者の端末である。ディジタル情報２は著作権権利者又は販売者（以

下、販売元という）固有の情報で暗号化された映像、音楽又は著書などである。暗号化情報生成器３はディジタル情報を販売元固有の情報で公開かぎ方式や共通かぎ方式などの暗号方式により対象データを暗号化する。販売元所有のＩＣカード（以下、販売元カードという）４は、販売元固有の情報や電子マネー情報が少なくとも格納されている。販売元ＩＣカード制御装置５は販売元カード４の情報を読み書きするためもので、通常、販売元カード４がこの販売元カード制御装置５に装着されているものとする。利用者所有のＩＣカード（以下、利用者カードという）６は、利用者固有の情報や電子マネー情報が格納されている。利用者カード制御装置７は、ディジタル情報販売装置１に内蔵されており、利用者カード６の情報の読み書き制御を行う。ディジタル情報を利用者が購入する場合、この利用者カード制御装置７に利用者カード６を装着する。販売履歴メモリ８はディジタル情報の販売履歴の情報を記憶するためのものであり、販売したディジタル情報の名称、利用者カード固有の情報などを格納する。販売者側外部通信手段９は、ディジタル情報販売装置１と外部機器との通信を行うためのものであり、直接又は間接適に利用者所有の装置と接続かつ通信することが可能である。販売者側プログラム記憶手段１０は、ディジタル情報販売装置を構成する各手段を制御するため必要なプログラム情報を格納するためのであり、電子マネー情報を利用した決済を制御するプログラムなどが格納されている。販売者側外部入出力手段１１はディジタル情報販売装置１の処理結果の表示などを外部へ出力するための出力機能や、ディジタル情報販売装置１の処理を実行するために外部からキーなどの情報を入力するための入力機能を備えている。販売者ユニット制御手段１２はディジタル情報販売装置１を構成する各手段、暗号化情報生成器３、販売元カード制御装置５、利用者カード制御装置７等を制御する。ディジタル情報２は、利用者が所有するディジタルデータ格納媒体２３に記憶される。なお、ディジタル情報２はディジタル情報販売装置内の、不図示の記憶手段に記憶されている。

【００１３】

ディジタル情報制御装置１３は利用者が購入したディジタル情報を表示又は音声などにより利用するため装置である。暗号化情報再生器１４は、暗号化されたディジタル情報を利用するために必要な複合処理を行う。第１利用者カード制御

装置１５は、第１利用者カード制御装置に内蔵され、利用者カード６の情報に対して読み書き制御を行う。第２利用者カード制御装置１６は、利用者カードの情報に対して読み書き制御を行う。ディジタル情報格納媒体制御装置１７は、ディジタル情報を格納した記憶媒体２３を装着して、この媒体からディジタル情報を読み出す。１８はディジタル情報制御装置固有の情報を格納するためのディジタル情報制御装置情報記憶手段である。利用者側プログラム記憶手段１９はディジタル情報制御装置を構成する各手段を制御するために必要なプログラム情報を格納する。ディジタル情報再生手段２０は、複合化されたディジタル情報の表示、出力などを行う。利用者側入出力手段２１は、ディジタル情報制御装置１３の処理結果の表示などを行うための出力機能を備え、また、ディジタル情報販売装置１の処理を実行するために、外部からキーなどの情報を入力するための入力機能を備える。販売者ユニット制御手段２２は、ディジタル情報制御装置を構成する各手段、暗号化情報再生器１４、第１利用者カード制御装置１５、第２利用者カード制御装置１６等を制御する。利用者側外部通信手段２３はディジタル情報制御装置１３と外部機器との通信をするためのものであり、直接又は間接適に利用者所有の装置との通信が可能である。

【００１４】

なお、販売者側プログラム記憶手段１０には、利用者へ秘密かぎ情報を販売するときに利用者の記憶媒体へ格納する秘密かぎ制御プログラムが格納されている。秘密かぎ情報制御プログラムは、秘密かぎの複製の制御や、販売者エリアからの利用料金の回収などを制御するものであり、ディジタル情報制御装置１３においても機能するものである。

【００１５】

図２に、販売元と第１利用者との販売手順を示す。第１利用者がディジタル情報販売装置１が設置されているディジタル情報販売店で、ディジタル情報を購入する際の、主にディジタル情報販売装置１の処理動作を述べる。なお、図２には示していないが、利用者が販売を希望するディジタル情報２を、第１利用者所有の記憶媒体２３に格納させる。これは、次に述べる料金の支払い前や秘密かぎ情報（キー情報）の格納前に行ってもよいが、料金支払い後や秘密かぎ情報の格納

後が好ましい。

【００１６】

まず、第１利用者が所有する利用者カード（以下、第１利用者カードという）をディジタル情報販売装置１内蔵の利用者カード制御装置７に装着する。

第１利用者のディジタル情報記憶媒体販売者ユニット制御手段１２は利用者カード制御装置７からカード挿入を示す情報を取得して（２００）、販売するディジタル情報の料金に相当する電子マネー情報を第１利用者の利用者カードから徴収する（２０１）。この電子マネー決済では利用者カードから販売元カードへ上記の電子マネーが移動することになり、利用者カードに格納される電子マネーが減算され、販売元カードに格納される電子マネーが加算される。ただし、この電子マネーの加減算については、単にデータの読み出しとその値に対する加減算を行うのではなく、販売者側プログラム格納メモリ１０に記憶される電子マネー制御プログラム及び利用者カードと販売元カードに内蔵されて記憶されている同電子マネー制御プログラムにより、プロトコル、通信データの暗号処理、また、販売元カードと利用者カード固有の情報を利用した認証処理を行い、セキュリティを担保させる。

【００１７】

更に、図示していないが、第１利用者カードの電子マネーが記憶されているエリアを、第１利用者が使用できる電子マネー格納エリアと販売元に使用が限定される電子マネー格納エリアに分割する。この販売元にのみ使用が限定される電子マネー格納エリアは、後述の利用者間でのディジタル情報のやりとりの際、ディジタル情報の購入料金として徴収する電子マネー情報を管理するために作成される。

【００１８】

利用者カードより販売元カードへのディジタル情報購入料金の徴収が完了した場合（２０１－ｙｅｓ）、利用者カードから第１利用者固有の情報を取得する（２０２）。この時、ディジタル情報の販売履歴を管理するために上記販売履歴メモリ８へ、取得した第１利用者の情報とディジタル情報の情報（例えば、ディジタル情報登録名、販売価格、販売日時、購入者名、購入者ＩＣカード番号など）

を関係付けして格納する。この情報管理により購入者からのクレームの対応や販売実績、又は購入者の傾向などを解析、管理することができる。また、ここでは第１利用者の秘密かぎ情報により復号化可能な暗号化の基になる情報（以下第１利用者暗号化情報）を少なくとも取得することにする。第１利用者暗号化情報は、利用者毎、あるいはカード毎に異なる情報であり、例えば、Purse ID（Personal ID）等の情報である。

【００１９】

次に、取得した第１利用者暗号化情報を基に、ディジタル情報を復号化するために必要な販売元固有の秘密かぎ情報を暗号化する。この暗号化処理は販売者ユニット制御手段１２から第１利用者暗号化情報と販売元固有の秘密かぎ情報を暗号化情報生成器３に渡し、暗号化情報生成器３により、販売元固有の秘密かぎ情報を暗号化する（２０３）。このような処理を行うことにより、ディジタル情報を利用するための販売元固有の秘密かぎ情報が第１利用者固有の情報に基づいて暗号化されているため、暗号化されたディジタル情報が複製され、更に、暗号化された販売元固有の秘密かぎ情報が利用者カード以外の利用者カードに複写されたとしても、販売元固有の秘密かぎ情報は第１利用者暗号化情報を有しない利用者カードを使用しても複号化できない。従って、ディジタル情報の不正な複製による使用を制限することができる。

【００２０】

また、このとき、利用者間における販売元固有の秘密かぎ情報の複写の際の制御や、販売者エリアの料金の回収を行う秘密かぎ情報制御プログラムを、利用者カードに併せて書き込む。

【００２１】

続いて、この暗号化情報生成器により暗号化した販売元固有の秘密かぎ情報を利用者カード制御装置７を用いて第1利用者カード６内部に書き込み（２０４）、第１利用者が希望するディジタル情報の販売処理を終了する。ディジタル情報の販売処理において、購入者への操作の手順などを上記販売者側外部入出力手段１１にディスプレイを接続して表示したり、購入者が不正なＩＣカードを利用した場合などのエラー処理を同じように販売者側外部入出力手段１１へスピーカー

を接続して、販売元及び購入者に通知するようにしても良い。

【００２２】

また、上述の例においては、決済を電子マネーにより実施する形態を説明したが、紙幣、硬貨などの現金で支払いを行ってもよい。

【００２３】

次に、図３を用いて、第１利用者が購入したディジタル情報を利用する場合の手順を説明する。

まず、販売元より上記で説明した手順により購入した、ディジタルデータ格納媒体２３に記憶されたディジタル情報２を、利用者のディジタル情報制御装置１３に内蔵されるディジタル情報格納媒体制御装置１７に装着する。ディジタルデータ格納媒体２３をディジタル情報格納媒体制御装置１７に装着すると、利用者ユニット制御手段２２でディジタル情報が装着されたことを検出する（３００）。このディジタル情報の装着状態の検出や以下に記述する処理については、利用者側プログラム格納メモリ１９に記憶されるユニット制御プログラムによって制御される。

【００２４】

次に、ディジタル情報からディジタル情報制御装置１３を介してディジタル情報固有の情報（ここでは、ＩＤ番号１７００とする。）を取得する（３０１）。この取得したＩＤ番号は暗号化されている情報である。ディジタル情報の装着状態とＩＤ番号の取得が完了すると第１利用者カード制御装置１５又は第２利用者カード制御装置１６へ利用者カードが装着されているかを判定する。第1利用者カードには、上述の暗号化された販売元固有の秘密かぎ情報が格納されている。なお、カード有無を判定する方法として、第１利用者カード制御装置１５、第２利用者カード制御装置１６に付加されるカード検出センサの状態を確認する方法や、利用者カード６に対してＩＳＯ７８１６に規定される条件で電源、クロック、リセットを供給して得られるＡＴＲ（Answer To Reset）の情報から確認する方法等がある。

【００２５】

利用者カード６の装着状態を検出すると（３０２）、利用者カード６に記憶さ

れている暗号化された販売元固有の秘密かぎ情報を取得するために、利用者ユニット制御手段が第１利用者カード制御装置を介して秘密かぎ情報の取得を行うためのコマンド情報を送信する。利用者カード６ではコマンド情報を受けた後、販売元固有の秘密かぎ情報をレスポンス情報として送信する。また、暗号化された販売元の秘密かぎ情報を復号化するために利用者カード固有の情報（第１利用者の秘密かぎ情報）を併せて送信する（３０３）。

【００２６】

販売元固有の秘密かぎ情報と第１利用者固有の秘密かぎ情報をレスポンスとして受信した利用者ユニット制御手段は、暗号化情報再生器１４に、販売元固有の秘密かぎ情報と第１利用者固有の秘密かぎ情報を送信して（３０４）、販売元固有の秘密かぎ情報を復号化させる（３０５）。ここで、暗号化情報再生器１４では、規定の暗号形式で暗号化した際に利用した第１利用者固有の秘密かぎ情報を入力情報とし、逆関数による計算を行い、複号化した販売元固有の秘密かぎ情報を利用者ユニット制御手段２２へ出力情報として返す（３０６）。販売元固有の秘密かぎ情報を受信した利用者ユニット制御手段２２は、暗号化情報再生器１４からレスポンスにより、再びディジタル情報格納媒体制御装置１７に装着されているディジタル情報にアクセスして再生用情報部分のデータを取得する。この再生情報部分のデータは、暗号化されていて、このままでは利用できない。したがって、再生情報部分の複号化のためには、販売元固有の秘密かぎ情報が必要となる。そこで、先に取得した販売元固有の秘密かぎ情報と、この再生情報部分のデータを暗号化情報再生器１４に送信して（３０７）、再生情報部分に付加されている暗号部分を解除した再生情報をレスポンスとして取得する（３０８）。

【００２７】

続いて、この再生情報をディジタル情報再生手段２０においてデータ変換処理やデータ圧縮状態を解凍する処理を行い（３０９）、その出力を利用者側入出力手段２１へ入力することでディジタル情報の映像、音楽などの情報としての利用を可能とする（３１０）。なお、この複号化は、ディジタル情報の再生する毎に行うものとする。ここで、利用者側入出力手段２１はディジタル情報制御装置に内蔵されるもので、外部からのモニタリングは不可能な構成とする。例えば、無

理にディジタル情報再生手段２０と利用者側入出力手段２１の間の信号をモニタリングした場合、あらかじめ組み込んであるモニタリング防止機能が動作してディジタル情報再生手段２０の動作を禁止する構成とする。なお、ディジタル情報の再生処理において、利用者への操作の手順などを上記利用者側入出力手段２１に表示したり、利用者が不正なＩＣカードを利用した場合などのエラー処理を同じように利用者側入出力手段２１の音声出力部により利用者に通知するようにしても良い。

【００２８】

また、履歴情報として、ディジタル情報の再生処理の各シーケンスをディジタル情報制御装置情報記憶手段１８に格納する。履歴情報は、不正処理に対する追跡用情報や、故障、システムエラーなどが発生した場合のメンテナンス用情報として利用することができる。利用者側外部通信手段２３を介して、ディジタル情報制御装置１と外部機器とを接続することにより、オンラインによる通信が可能となる。利用者側外部通信手段２３を利用し、故障、システムエラーの発生した場合の装置側の対策情報をオンライン経由で販売元の装置から送信すれば、リアルタイムの修復を行うことが可能となる。

【００２９】

次に、図４を用いて、本実施例の特徴である、第一利用者から第二利用者（直接、販売元からディジタル情報の購入をしていない利用者）へのディジタル情報複写手順について、説明する。そして、図５を用いて、第１利用者所有及び第２利用者所有のＩＣカード（以下第２利用者カードとする）の詳細な構成について説明する。

本実施例においては、キー情報の複写は、第１の記憶媒体に記憶された秘密かぎ情報プログラムに従って、図１のディジタル情報制御装置１３が行う。また、ディジタル情報２については、ディジタルデータ格納媒体２３から、不図示の第2の利用者のディジタルデータ格納媒体に複製させることとする。ディジタルデータ２の複製は、いつ行ってもよいが、以下の販売者格納エリアに販売させた後や、販売元固有の秘密かぎ情報を第２の利用者のＩＣカードに書きこんだ後が好ましい。

【００３０】

まず、第１利用者カード制御装置及び第２利用者カード制御装置１６に第１利用者と第２利用者のＩＣカードをそれぞれ装着することにより、複写処理を開始する。両者のＩＣカードが各利用者カード制御装置へ装着される（４００）と、利用者ユニット制御手段は電源、クロック信号、リセット信号を第１利用者カードと第２利用者カードの入出力部３０及び４０へ供給する（４０１）。

【００３１】

続いて、第１利用者カードから、ディジタル情報の購入履歴と、ディジタル情報を利用するための販売元固有の秘密かぎ情報を格納している履歴とを示す購入履歴情報をレスポンスとして返信する。この購入履歴情報は第1利用者カードに内蔵される履歴格納メモリ３１から取得される。また、第１利用者カードから、購入履歴情報と併せてディジタル情報を購入するための価格情報を返信する。価格情報は、先のディジタル情報販売処理により第1利用者カード１に書き込まれた制御プログラム（秘密かぎ情報制御プログラム格納メモリ３３に格納）に格納されている。これら２つの情報（購入履歴情報、価格情報）を利用者ユニット制御手段が受信する（４０２）と、金額徴収のシーケンスへ遷移する。

【００３２】

続いて、第２利用者カードに対して、電子マネー情報を取得するためのコマンドを第２利用者カード制御装置１６を介して第２利用者へ送信して、第２利用者カードよりＩＣカード内の残金を示す残金情報をレスポンスとして取得する（４０３）。続いて、残金情報により価格情報を満足する残金が第２利用者カードにあると判定すると（４０４－ＹＥＳ）、第2利用者のＩＣカード内の電子マネー格納メモリ４６に、販売元が唯一アクセス可能な販売者専用エリア４６－２を作成して（４０５）、価格情報に相当する電子マネー情報を販売者専用エリア４６－２へ格納する（４０６）。結果として、第２利用者が使用できるエリア４６－１から価格情報相当分の電子マネー情報を減額して、販売者専用エリア４６－２へ価格情報相当分の電子マネー情報を増額することになる。ただし、この電子マネーの加減算については、単にデータの読み出しとその値に対する加減算を行うのとは異なり、第２利用者カードに記憶される電子マネー制御プログラム（電子

マネー制御プログラム格納メモリ４７に格納される）によりプロトコル、通信データの暗号処理、また、第２利用者固有の情報を利用した認証処理を行いセキュリティ面で充実した処理を行う。

【００３３】

続いて、第２利用者カードから第２利用者固有の暗号化情報を、第２利用者カードのロック管理メモリ４５から取得して（４０７）、第２利用者固有の暗号化情報を第１利用者カードに送信する（４０８）。この後、第１利用者カード内部において、受信した第２利用者固有の暗号化情報をもとに、販売元固有の機密かぎ情報の再暗号化処理を行う。手順としては、第１利用者のＩＣカード内の販売者秘密かぎ暗号化情報エリア３４－２に格納の暗号化された販売元固有の秘密かぎ情報と、第１利用者秘密かぎエリア３４－１に格納の第１利用者秘密かぎ情報を、第１利用者カードの演算手段３８が取得して、第２利用者より取得した第２利用者暗号化情報を併せて、暗号化又は復号化処理を行うための販売元固有の秘密かぎ情報を、暗号復号化処理手段３２へ送信する（４０９）。次に、秘密かぎ情報暗号復号化処理手段３２では第２利用者暗号化情報で販売元固有の秘密かぎを暗号化する。ここでは、第１利用者秘密かぎで販売者秘密かぎに施されている暗号化情報を解除した後、第２利用者暗号化情報により販売者秘密かぎを暗号化する。この結果として、第２利用者秘密かぎで復号可能な暗号化された販売者秘密かぎが生成される（４１０）。このように、秘密かぎ情報の暗号化と復号化処理をＩＣカード内部で処理させることにより、外部からのモニタリングやデータの改ざんなどの不正アクセスに対するセキュリティを担保することができる。

【００３４】

次に、第2の利用者暗号化情報に基づき暗号化された販売元固有の秘密かぎ情報をレスポンスとして、利用者ユニット制御手段が受信して、第２利用者内の暗号化された販売者秘密かぎを格納するためのエリア４４－２へ、第２の利用者暗号化情報に基づき暗号化された販売元固有の秘密かぎ、を書き込む（４１１）。また、このとき、利用者間における販売元固有の秘密かぎ情報の複写の際の制御や、判愛社エリアの料金の回収を行う秘密かぎ情報制御プログラムを、第２の利用者カードに併せて書き込む。

【００３５】

ステップ４１１の手続において、販売者秘密かぎが書き込まれたことを示す情報を、履歴格納メモリ４１へ格納することにより、この情報を利用して不正な複写を取り締まる。また、複写の回数や販売元から数えて何回目の複写になるか等を書きこむこととすれば、世代管理が可能となる。販売元固有の秘密かぎ情報の複写処理を制御するプログラムに、世代管理を行うための情報を反映させて複写に関する限定を付加するようにしても良い。

【００３６】

なお、複写処理を開始する際、必ず利用者に対して、“この情報の複写は有償です。”の旨を表示または通知することで、利用者の意思で複写処理が行われたことを確定する方式を採用するとよい。

【００３７】

上記処理により第１利用者から第２利用者への第２の暗号化販売者秘密かぎの複写及び購入料金を、第２利用者のＩＣカード内の販売者専用エリアへの格納ができたことになる。

【００３８】

なお、上記説明では、「複写」処理について記述した。複写処理により、第1利用者と第2利用者の両方に販売元秘密かぎが存在することになる。しかし、第2の利用者に書くのエリアにのみ販売元秘密かぎが存在し、第1利用者の格納エリアには販売元秘密かぎが秘密かぎが存在しない秘密かぎの「移動」処理を行わせてもよい。移動処理を行うためには、第２利用者への秘密かぎ情報の書き込み完了時点で、第１利用者カード内の販売者秘密かぎ格納エリア３４－１に格納される、第２の暗号化販売元秘密かぎ情報を消去すればよい。つまり、複写処理は、秘密かぎが増加する処理であり、個人間の転々流通を利用して販売の拡大を目的とする場合に有効な方法である。一方、移動処理は、秘密かぎが移動処理によっては増加せず、販売字にその総数が決まる“限定発売“の形態でディジタル情報を配信するような場合に有効な方法である。

【００３９】

本実施例によれば、履歴を記録することとしたため、販売元から利用者への直接

的に販売した絶対数を管理することが可能となる。市場に提供する利用可能なディジタル情報の総数管理を販売元により一元化する場合に有効である。

【００４０】

なお、本実施例においては、販売元固有の秘密かぎ情報を、それぞれ第１の利用者固有の秘密かぎ情報や、第2の利用者固有の秘密かぎ情報で暗号化する、高度なセキュリティを持つ例を説明した。しかし、これに限らず、販売元固有の秘密かぎ情報を利用者固有の秘密かぎ情報で暗号化しなくても、本実施例の効果を有するものとなる。

【００４１】

また、本実施例においては、ディジタルデータ２を利用者のディジタルデータ格納媒体２３に記憶させる構成としたが、利用者カード６に秘密かぎ情報と共にディジタルデータ２を記憶させてもよい。

【００４２】

また、利用者カード６に、販売元固有の秘密かぎ情報を記憶させることとしたが、ディジタルデータ格納媒体２３に、ディジタルデータ２と共に、販売元固有の秘密かぎ情報を記憶させてもよい。

【００４３】

なお、本実施例において、販売元固有の秘密かぎ情報の複製の際に、販売者エリアへ販売金額を格納させることを説明した。このような制御は秘密かぎ情報制御プログラムに規定されている。秘密かぎ情報制御プログラムは、ディジタル情報販売装置１がディジタル情報の販売と共に利用者カードに書きこまれる。なお、上述のように、秘密かぎ情報制御プログラムをディジタルデータと共に、ディジタルデータ格納媒体に記憶させてもよい。秘密かぎ情報制御プログラムは、当然、販売元固有の秘密かぎ情報の複製時に第２の利用者のカードや媒体に記憶される。また、秘密かぎ情報制御プログラムをディジタルデータの複製時に複製させるのではなく、販売元固有の秘密かぎ情報の複製時に販売者エリアへ販売金額を格納させる制御機能を、ディジタルデータ制御装置１３に予め持たせておいてもよい。　次に、図６、図７を用いて、販売者エリア４６－２に格納された販売金額（電子マネー情報）を回収する方法を説明する。あわせて、第２、第３・・

第ｎ利用者間の購入金額に相当する電子マネー情報の移動方法を説明する。

まず、図６において、販売店５０はディジタル情報の販売元である。ディジタル情報５１は暗号化が施されていないディジタル情報である。販売元固有の暗号化情報５２は、販売するディジタル情報５１を販売元固有の暗号化情報で暗号化する。販売元固有の秘密かぎ情報５３は、データの復号化の際に利用ものである。販売元が所有するＩＣカード５４は、利用者から購入料金（電子マネー）を格納することなどに利用する。ディジタル情報５５は販売元の暗号化情報５２で暗号化され情報である。利用者については、第１、第２、第３、第Ｎ利用者について記述する。第１利用者６０は、販売元からディジタル情報５５を購入する。第１利用者固有の秘密かぎ情報６１は、同利用者の暗号化情報でありる。同利用者所有のＩＣカード６３には、電子マネー情報が少なくとも格納されているものとする。情報６４は販売元固有の秘密かぎ情報を第１利用者固有の暗号化情報で暗号化されたものであり、この情報を購入する場合、第１利用者は第１利用者固有の暗号化情報を販売元に渡すことでこの情報が作成される。なお、第２、第３利用者及び第Ｎ利用者に対する構成は第１利用者と同様な構成となっている。ただし、販売元固有の秘密かぎ情報７４は第２利用者固有の暗号化情報により第１利用者カード内で暗号化された情報であり、販売元固有の秘密かぎ情報８４は第３利用者固有の暗号化情報により第２利用者カード内で暗号化された情報であり、販売元固有の秘密かぎ情報９４は第Ｎ利用者固有の暗号化情報により第Ｎ－１利用者カード内で暗号化された情報である。

【００４４】

販売元と第１利用者間の販売手順及び第１利用者と第２利用者との複写処理については、先に説明した手順により行うものとして、ここからは第２利用者から第３利用者及び第Ｎ利用者までの複写処理とその際に発生する料金の遷移状態について説明する。

第２利用者から第３利用者へのディジタル情報５５の複写に伴い、第３利用者はこの情報を利用するために、販売元固有の秘密かぎ情報が必要となる。この場合、ディジタル情報５５自体は販売元固有の暗号化情報で暗号化されているので複写をすることにはなんら問題はない。また、暗号化された販売元固有の秘密か

ぎ情報を複写しても暗号化されていて、販売元により許可された利用者以外がこの情報を取得しても利用できないので、これもまた問題はない。

【００４５】

さて、第３利用者固有のＩＣカードに第２利用者と同様に販売元固有の秘密かぎ情報７４を複写することがディジタル情報を販売元から購入したということになり、第一利用者と同様に購入料金の支払が発生する。先の例によれば、第２利用者においても第１利用者から上記秘密かぎ情報７４を購入した際、購入料金に相当する電子マネー情報が徴収されていることになっている。

【００４６】

そこで、図７を用いて、第３利用者カードについて、カード内に格納されている電子マネー情報の販売元との関係を説明する。まず、第３利用者から料金（ここでは購入料金を￥１００とする）を徴収する（７０１）。この購入料金は電子マネー情報の移動により成立する。実際には第３利用者が所有するＩＣカード８３の電子マネー情報格納メモリに販売元専用エリアを作成して、この販売元専用エリアに購入料金に相当する電子マネー情報を移動させる。これは、図５を用いて説明したものと同様な構成とする。また、料金徴収の例を述べると、第３利用者のＩＣカード８３に￥５００格納されていて、料金￥１００がこのエリアから引き出されて、新しく作成した販売元専用エリアに￥１００が追加格納される。この時、電子マネー情報の増減については結果として各エリアの電子マネー情報に対して加減算が行われたようになるが、実際は暗号化データに対する計算処理を行い、高いセキュリティに保護されて実行されているものである。

【００４７】

購入料金が徴収完了する（７０２－ｙｅｓ）と、次に第３利用者の暗号化情報８２を取得する（７０３）。そして、第３利用者の暗号化情報８２と第２利用者の秘密かぎ情報７１及び第２利用者の暗号化情報７２で暗号化された販売元固有の秘密かぎ情報７４との３つの情報により第３利用者の暗号化情報８２で暗号化された販売元固有の秘密かぎ情報８４を作成する（７０４）。次に、第３利用者の暗号化情報で暗号化された販売元固有の秘密かぎ情報８４を第３利用者のＩＣカードへ書き込む（７０５）。この情報の書き込みが完了することで第３利用者

はディジタル情報５５を利用できることになる。以上の動作は、図４で示した第２の利用者への複写と同様である。

【００４８】

ここで、ディジタル情報購入料金について考えてみると、第３利用者への複写処理が半ば完了した時点で、第２利用者及び又は第３利用者の各々のＩＣカードに販売元専用の電子マネー情報が格納されていることになる。この販売元が回収すべき購入料金（電子マネー情報）を効率良く回収するために、後続の利用者が希望する複写（販売元固有の秘密かぎ情報の複写）とリンクさせて、後続の利用者のカード内に電子マネー情報を移動させる。

【００４９】

つまり、第３利用者の複写元となる第２利用者に販売元専用電子マネー格納エリアが存在することになる。そして、対象となるエリアの電子マネー情報の格納状態を確認する（７０６）。第２利用者のＩＣカードに購入料金がある（７０６－ｙｅｓ）場合は、第２利用者のＩＣカードから対象となる電子マネー（購入料金相当）を第３利用者のＩＣカードへ格納する（７０７）。ここでの電子マネー情報の移動に関しては、先に第３利用者のＩＣカード内に格納した販売元専用のエリアへ電子マネー情報をセキュリティに保護されて格納することになり、結果として、第３利用者の販売元専用の電子マネー格納エリアの電子マネー情報が加算されたことになる。以降第３利用者から第４利用者の複写処理及び後続の利用者間の複写処理ついても第２利用者から第３利用者への上記購入料金が移動と同様の手順で行われる。最後にディジタル情報とその利用に必要な販売元固有の秘密かぎ情報の複写に関して、第ｎ－１利用者と第ｎ利用者（最終複写先となる利用者）間の複写処理が終了する（７０８－ｎｏ）と上記手順で第ｎ利用者のＩＣカードの販売者専用エリアに格納された購入料金ｘは、下記に示す式で計算することができる。

【００５０】

ｘ＝ディジタル情報の購入料金×（ ｎ－１ ）　　（ただし２≦ｎ）

本実施例において、最終複写先を第８利用者とし、また、ディジタル情報の購入料金を一律１００円と仮定すると上記手順により第８利用者への複写処理が完了

時点で、販売元が徴収可能な電子マネーは総額７００円となり、これが第８利用者のＩＣカードに格納されている。

【００５１】

第８利用者から販売元が蓄積された購入料金を回収する方法として、第８利用者のディジタルデータ制御装置がオンラインの環境下で稼動する場合、第８利用者が対象となるディジタル情報を利用する時点で、第８利用者カードに記憶されている購入料金回収プログラム（第７利用者から第８利用者や販売元固有の秘密かぎ情報の複写の際、同様に第８利用者カードへ書き込まれているものとする。）により格納されているすべての料金をオンラインで販売元所有のＩＣカード５４へ移動させることで回収できる（７０９）。

【００５２】

また、第８利用者のディジタル情報制御装置がオフラインの環境下で稼動する場合、購入料金回収プログラムにより第８利用者に対して、販売店へＩＣカードを持参すると蓄積された料金に対応して返金サービスが受けられるなどの情報を通知することで蓄積された購入料金の回収経路を確保することができる。また、返金サービスの他にも最新の情報をＩＣカードを利用して提供するなどのサービスを行うことで、より一層高い回収率が望めることになる。また、秘密かぎ情報はディジタル情報個々に異なるものなので、複数のディジタル情報を利用する場合、各秘密かぎ情報に対して販売元専用の電子マネー情報格納領域へ個別に格納すると購入料金回収時の処理に対して利便性が向上する。また、販売元固有の秘密かぎ情報の格納メモリの制約により、複写のためのメモリ容量が不足する場合には、その旨を利用者に通知するようにしても良い。なお、本実施例においては、第８利用者がオンラインにより販売元エリアの金額を送付することを説明したが、第２利用者がこれを行ってもよいことはいうまでもない。

【００５３】

上記の実施例においては、販売元固有の秘密かぎ情報と購入料金に相当する電子マネー情報がリンクして移動する場合について説明した。次に、利用者の動作環境を示す情報と販売元との過去の取引履歴を示す情報を利用することで、オフラインの環境下に蓄積される購入料金の移動を更に効率良く回収する方法につい

て、図８、図９及び図１０を用いて説明する。

図８は販売元及び販売元からディジタル情報を購入した第１利用者から第ｎ利用者までのディジタル情報制御装置の環境を示したものである。ディジタル情報販売装置１００は回線に接続され外部との通信機能を少なくとも備えるディジタル情報販売装置１であり、販売元が管理するものである。ディジタル制御装置１０１、１０４、１０８、１０９は利用者が所有する装置であり、これには回線に接続され外部との通信機能を少なくとも備えるものとする。また、ディジタル情報制御装置１０２、１０３、１０５、１０６、１０７は利用者が所有する装置であり、これには回線に接続され外部との通信機能はないものとする。また、ディジタル情報販売装置１００を含め、１０１から１０９までの各装置を所有する利用者及び販売者はＩＣカードを所有していて、その中には電子マネー情報、購入履歴情報などが格納されているものとする。ただし、購入履歴に関する情報は販売元と直接的な取引が行われた場合に記憶されるものとする。１１０は、各装置が接続する回線であり、電話回線、専用回線などである。

【００５４】

まず、第１利用者と販売元におけるディジタル情報の販売において、先の実施例で説明した方法により販売元固有の秘密かぎ情報を、第１利用者のＩＣカードに書き込む際、購入時刻や販売元の利用回数を示す情報を第１利用者のＩＣカードの履歴格納エリアに、一緒に書き込む。ここで書き込む内容について図９を用いて説明する。

【００５５】

なお、ここでは第１利用者カードの内容を例にして説明する。ディジタル情報の購入した日付情報を格納するための購入日格納エリア１２５－１に購入日に関する情報として、年月日、時刻を書き込む。この情報は販売元との最新取引を管理するものとして取り扱うため、販売者と利用者間の取引では必ず記録ヲ行うこととする。ただし、元の購入日を新しい情報に更新する形式としても良いし、新しい購入日を追加する形式としても問題ない。また、上記購入日の書き込みと同様に販売元の利用回数を示す情報を書き込むための利用回数エリア１２５－２に販売元と第１利用社の取引が行われる毎に利用回数を更新（カウントアップ）す

る。なお、販売元との取引については、第１利用者のようにオンライン環境下で稼動可能な端末の場合、ディジタル情報の配信と購入料金決済（電子マネー情報による）及び販売元固有の秘密かぎ情報の書き込みをオンラインでリアルタイムに実行しても良い。また、販売元（販売店など）まで出向いて、そこで上記情報の書き込み処理を含む取引を行っても良い。販売元と利用者間の取引については、確実に購入料金を回収可能であるが、この後、第１利用者以降第ｎ利用者までの購入料金をいかに回収するかが問題となる。そこで、第１利用者から第２利用者への複写処理で徴収される購入料金の遷移の仕方を基本として、以降第ｎ利用者までの購入料金の遷移をＩＣカードに格納される購入来歴情報により制御する方法について説明する。

【００５６】

第１、第２利用者間で販売元固有の秘密かぎ情報を複写するための複写処理は、第１利用者又は第２利用者の環境下で行う。すなわち、第２利用者のＩＣカードに格納され、かつ、第２利用者専用エリアに格納される電子マネー情報から販売元専用エリアに購入料金相当の電子マネー情報を格納して、次に、第１利用者固有の暗号化情報で暗号化された販売元固有の秘密かぎ情報を第２利用者固有の暗号化情報により暗号化された販売元固有の秘密かぎ情報という形式にするため暗号化及び復号化処理を行う。そして、この情報を第２利用者のＩＣカードに書き込む。一連の処理を行った後、第１利用者及び第２利用者のＩＣカードから購入来歴情報を取得する（１０００）。この処理で取得可能な情報として、購入日格納エリア１２５－１に格納される購入日情報と利用回数エリア１２５－２に格納される利用回数情報の２つであり、第１、第２利用者に対するこの２つの情報を比較して、電子マネー情報を移動させることになる。ここでは、比較条件を購入日情報に限定し、かつ、両者の購入日情報により古い日付から新しい日付のＩＣカードの方向へ上記購入料金を移動させることにする。１０００で取得した購入日情報を西暦により取扱い全部で７バイトのデータで定義する（年を示す値に２バイト、月を示す値に１バイト、日を示す値に１バイト、時間を示す値に１バイト、分を示す値に１バイト、秒を示す値に１バイトを割り当てる）と第１利用者の購入日が１９９９年０３月０１日１３時００分００秒の場合（１００１－ｙ

ｅｓ）、

Ｈ‘１３６３０３０１０Ｄ０００００（１６進数表記）

として取り扱う。また、販売元との直接的な取引がない場合（１００１－ｎｏ）、そのＩＣカードには購入日情報がないので、

Ｈ’ＦＦＦＦＦＦＦＦＦＦＦＦＦＦＦＦ（１６進数表記）

として値を代用する（１００２）。この条件により、第ｎ－１利用者の購入日情報をＸ１、第ｎ利用者の購入日情報をＸ２とすると、Ｘ１≦Ｘ２の場合、両者のＩＣカードに格納される購入料金の全額を第ｎ－１利用者のＩＣカードへ格納する。図８の例では第１利用者には購入日情報（１９９９年３月１日）があり、第２利用者には購入日情報がないので、この場合、第１利用者のＩＣカードに購入料金が格納される。上記の方法で第２利用者以降第ｎ利用者までの利用者間の複写処理を繰り返し行う（１００６－ｙｅｓ）。最後の第ｎ利用者と第ｎ－１利用者間の複写処理が終了する（１００６－ｎｏ）と結果として購入日情報が格納されているＩＣカードへ購入料金が格納されていくことになる。また、購入日情報の代わりに利用回数情報の順位を優先して、利用回数の多い方向へ移動させることにしても良い。ただし、この場合、販売者と直接取引がない場合の利用回数情報をＨ‘００（１６進数表記）で取扱い、第１利用者の利用回数情報をＹ１、第２利用者の利用回数情報をＹ２とすると、Ｙ１≧Ｙ２の場合、両者のＩＣカードに格納される購入料金の全額を第１利用者のＩＣカードへ格納する。このように販売元との直接的な取引があり、かつ、その取引が最近に確立された又は利用頻度の多いＩＣカードへ購入料金を移動させることで、販売元への回収率がより一層向上する。

【００５７】

更に購入料金の回収状況を向上させる方法として、図９のプロバイダ契約情報格納メモリに格納される情報により購入料金の移動を制御する方法が考えられる。すなわち、第１利用者から始まる利用者間の複写処理のリングの中でオンライン環境下で稼動する装置の利点を活用して、オフライン環境下で稼動する装置を所有する利用者間で蓄積された購入料金を一括して販売元に送信（回収させる）する方法である。この方法は上記で説明した購入日情報及び利用回数と組み合わ

せて実施しても良いし、プロバイダ契約情報格納メモリ１２４に格納される情報に特化して実施しても良い。ここでは組合せによる実施例について下記に述べるが、前提条件として、利用者がインターネットなどのネットワーク上に配信される情報を利用者する環境の情報として、ネットワークにアクセスするためのサーバを提供する会社名やその連絡先を示す電話番号又はサーバ固有の番号などを格納するためのプロバイダ契約情報格納メモリ１２４にあらかじめ各種情報（以下プロバイダ情報）を格納してあるものとする。また、第ｎ利用者のＩＣカードに格納され、かつ第ｎ利用者専用エリアに格納される電子マネー情報から販売元専用エリアに購入料金相当の電子マネー情報を格納して後、第ｎ－１利用者固有の暗号化情報で暗号化された販売元固有の秘密かぎ情報を第ｎ利用者固有の暗号化情報により暗号化された販売元固有の秘密かぎ情報という形式にするため暗号化及び復号化処理を行い、この情報を第ｎ利用者のＩＣカードに書き込むまでの一連の処理を行った後の処理について説明する。

【００５８】

まず、第ｎ－１利用者のプロバイダ契約情報格納エリアの情報を取得して、プロバイダ情報があれば（１１００－ｙｅｓ）、第ｎ－１利用者のＩＣカードに両者のＩＣカードに格納される購入料金をすべて格納する（１１０１）。もしも、第ｎ－１利用者のＩＣカードにプロバイダ情報が無い場合（１１００－ｎｏ）、第ｎ利用者のプロバイダ契約情報格納エリアの情報を取得して、プロバイダ情報があれば（１１０２－ｙｅｓ）、第ｎ利用者カードに両者のＩＣカードに格納される購入料金をすべて格納する（１１０３）。もしも、第ｎ利用者のＩＣカードにプロバイダ情報が無い場合（１１０２－ｎｏ）、両者の購入日情報を取得した（１１０４）後、この情報を比較する。第ｎ－１利用者の購入日情報をＸ１、第ｎ利用者の購入日情報をＸ２として、Ｘ１＜Ｘ２の場合（１１０５－ｙｅｓ）、第ｎ利用者側に格納する（１１０６）。なお、Ｘは日付が新しいほうが大きい数をもつものとする。Ｘ１＞Ｘ２の場合（１１０７－ｙｅｓ）、第ｎ－１利用者側に格納する（１１０８）。また、Ｘ１＝Ｘ２の場合、両者の利用回数情報を取得した（１１０９）後、この情報を比較する。第ｎ－１利用者の利用回数情報をＹ１、第ｎ利用者の利用回数情報をＹ２として、Ｙ１＜Ｙ２の場合（１１１０）、

第ｎ利用者側に格納する（１１１１）。上記以外の場合、第ｎ－１利用者側に格納する（１１１２）。この手続きを続ける場合（１１１３）は、Ｎに１を加え、ステップ１１００に戻る。また、購入日情報及び利用回数情報が書き込まれていない場合については、先に説明した手順で値を代入して比較することになる。

【００５９】

上記の手順で格納された購入料金の移動方向は、第１にプロバイダ情報があるＩＣカードに格納され、第２に複写した日に１番近い日に販売元と取引を行った履歴のあるＩＣカードに格納され、第３に利用回数が多く、販売元との取引確率の多いＩＣカードに格納されることになる。上記の購入料金が格納されたＩＣカードで、特に、プロバイダ情報が格納されているＩＣカードから購入料金を回収するタイミングは利用者がインターネットなどのネットワークにアクセスする際、あらかじめ記憶してある販売元の連絡先を示す電話番号に回線経由で自動的にダイヤリングしてアクセスを行い、回線経由で利用者のＩＣカードから購入料金に相当する電子マネー情報を全額を送信して、販売元のＩＣカードの電子マネー格納エリアに格納することで回収を完了する。この回線経由の通話料金については、販売元が負担するためフリーダイヤルなどを設定することで利用者に負担がかからないようにする。この方法によれば、オフライン環境下に埋もれてしまいがちな販売元が回収できる電子マネー情報を効率良く、かつ、高確率で回収できるようになる。

【００６０】

次に、利用者のＩＣカードなどに記憶媒体に複数のアプリケーションが格納されており、ディジタル情報の購入に直接関与しないアプリケーションを利用してディジタル情報の購入料金を回収する方法について説明する。

図１２は本実施例のシステムを示す構成図であり、ディジタル映像販売元１４０はディジタル映像などのディジタル情報を販売する。銀行ＡＴＭ１４１は銀行における引き出し、預け入れ、振り込みなどの処理が可能である。金額情報格納メモリ１４２は利用者の金額情報を格納する。利用者専用エリア１４２－１は利用者１が使用できる電子マネー情報を格納する。販売者専用エリア１４２－２は利用者１のＩＣカードにある販売元が購入料金を回収するためのエリアである。

銀行ＡＴＭ用ＡＰ１４３は利用者１のＩＣカード１３０にあり、電子マネーによる決済用ＡＰ、ポイント管理用ＡＰなどが格納されているＡＰメモリである。キー管理メモリ１４４はディジタル映像を再生するために必要なキー情報１４４－１が格納されている。また、第2の利用者カード１３１は、第１の利用者のＩＣカード１３０と同等の構成とする。

【００６１】

まず、ディジタル映像販売元１４０から利用者１は情報に対する支払を済ませると利用者１のＩＣカード１３２にあるキー管理格納エリア１４４へディジタル映像１４５を再生するためのキー情報１４４－１とディジタル映像１４５を書き込んでもらう。ここでディジタル映像はＩＣカードに格納せず、ＩＣカードと異なる別の記憶媒体に格納しても良い。ここでは、ＩＣカード内に格納することにする。利用者１ＩＣカードに格納されたディジタル映像１４５及びキー管理エリアに格納されたキー情報１４４－１により利用者１はディジタル映像１４５を生成することが可能になったことになる。次に、この利用者１から利用者２へキー情報１４４－１をコピーする際の手順では、利用者２の利用者専用エリア１４７－１からディジタル映像の購入料金（この場合３００円）の電子マネー 情報を販売元専用エリア１４７－２へ格納することでキー情報のコピーを許可する。ただし、この制御は利用者２のＡＰメモリ１４６に格納されている電子決済用ＡＰにより行われるもので、この電子マネーＡＰはキー情報１４４－１のコピー開始時に利用者１から利用者２へコピーされたものである。また、利用者１は販売元との決済時に利用者１のＡＰメモリ１４３に販売元よりコピーされたものである。購入料金として販売者エリアに電子マネーが格納されたことにより、キー情報のキー管理エリアへのコピーが許可されて、利用者２はディジタル映像１４５を再生可能な状態になる。ここでポイントとなるのは、キー情報のコピーに必ず販売元エリア１４７－２への電子マネー情報の格納動作が付随していることにある。

【００６２】

利用者エリア１４７－１における残金が不足している場合、このキー情報のコピーは禁止して、ディジタル映像１４５の再生を不可能にする。また、販売元専

用エリア１４７－２に格納された電子マネー情報は常に販売元固有の情報によりロック状態となっており、利用者２が利用しようとしても不可能である。このロック状態を解除するためには販売元固有の情報を入力することが必要である。このように電子マネー情報の格納処理やロック状態の制御などは電子決済用ＡＰにすべて準じて行われる。これらの動作は上述の実施例と同様である。

【００６３】

次に、利用者２の販売元専用エリア１４７－２に購入料金として格納された電子マネー情報の回収について図１３の手順を示すフローチャートにより説明する。利用者２のＡＰメモリには銀行ＡＴＭ用ＡＰが格納されていて、利用者２は銀行にて、このＩＣカード１３５を使って預金や引き出し及び振り込みなどが行えるものとする。ここで、利用者２が銀行ＡＴＭ１４１により振り込みを行うと、ＡＰメモリに格納される銀行ＡＴＭ用ＡＰが起動する（１３００）。この起動に関しては、ここでは図示せぬアプリケーション管理ＡＰが電子決済用ＡＰへ購入金額の格納の有無を確認した後、銀行ＡＴＭ用ＡＰを起動することにする。ここで、販売元専用エリア１４７－２に購入料金が格納されていると上記の確認で判明した場合（１３０１－ｙｅｓ）、電子決済ＡＰにより銀行ＡＴＭ１４１へ購入料金の全額を送金する（１３０２）。銀行ＡＴＭ１４１は購入料金を受け取ると、続いて購入料金を送金する販売元の連絡先を示す情報を利用者２ＩＣカード１３５より受け取る。この連絡先を示す情報も電子決済用ＡＰが制御して送信する。購入金額と販売元の連絡先情報を受け取った銀行ＡＴＭは即座に販売元と回線接続をして（１３０３）、利用者２から受け取った購入金額をすべて販売元１４０に送金する（１３０４）。送金が完了すると販売元１４０と銀行ＡＴＭ１４１間の回線接続を切断して（１３０５）、銀行ＡＴＭのサービスを実行する。このタイミングで利用者２のＩＣカード内でも電子決済ＡＰから銀行ＡＴＭ用ＡＰに切り替わり、振り込み処理が可能になる。利用者２の振り込み処理の終了時点では、既に販売元１４０への回収が完了したことになっている。

【００６４】

本実施例によれば、１枚のＩＣカードで複数のアプリケーションを利用できる構成として、ディジタル情報の再生以外（例えば、ショッピングや銀行振り込み

など）でＩＣカードを利用する際、バックグラウンド処理によりＩＣカードに蓄積された料金を販売元に振り込む方式を採用することで、利用者の意図する行動を利用した販売元と利用者間の料金回収ルートの拡張が可能である。

【００６５】

上記の実施例では、利用者の意図する振り込み処理の前に購入料金を販売元までの銀行ＡＴＭを経由してディジタルデータ販売元へ送金処理を行っているが、これを銀行ＡＴＭで一次保管して、利用者と銀行ＡＴＭ間の振り込み処理の終了時に改めて販売元へ送金するような形式の実施例について、その手順を図１４に示して説明する。

ディジタル映像１４５の購入料金を販売元専用エリア１４７－２へ格納してある状態で利用者２が銀行ＡＴＭを利用する場合、利用者２はＩＣカード１３５を銀行ＡＴＭ１４１に装着して振り込み処理を実行することになる。この時、アプリケーション管理ＡＰと銀行ＡＴＭ用ＡＰ及び電子決済用ＡＰの起動に関する関係は上記の例で説明したものと同様の動作となる。まず、銀行ＡＴＭ用ＡＰが起動されるが（１４００）、電子決済用ＡＰにより販売元専用エリア１４７－２の格納状況を確認して（１４０１）、購入金額が格納されている場合（１４０１－ｙｅｓ）、銀行ＡＴＭ１４１へすべての購入金額の送金と販売元の連絡先情報を送信して電子決済用ＡＰの処理を終了する（１４０２）。次に、利用者２の銀行ＡＴＭ用ＡＰと銀行ＡＴＭ間において振り込み処理を開始して（１４０３）、無事に振り込み処理を終了する（１４０４）と利用者２のＩＣカードを排出する。ここで、カード排出の時点では既に購入料金は銀行ＡＴＭへ送金されており、販売元への送金にはこのＩＣカードがＡＴＭに装着されている必要はない。続いて、銀行ＡＴＭは先に受け取った購入料金を確認して、販売元への送金がある場合（１４０５－ｙｅｓ）、販売元へ送金するために回線接続を行う（１４０６）、回線の接続を正常に完了すると電子マネーによる送金を開始する（１４０７）、送金を正常に終了した後、販売元１４０と銀行ＡＴＭ１４１間の回線接続を切断して販売元への購入料金の回収を完了する（１４０８）。上記において、回線接続に失敗した場合などは再度接続するようにしたり、回収のための電子マネー情報の送金時にエラーが発生した場合の再送金処理の実行を行うとより一層の信頼

性が得られるようになる。

【００６６】

上記例では、銀行ＡＴＭを利用して販売元へ利用者２の購入料金を送金することにしたが、買物の際に使用するクレジット用ＡＰで回収させるようにアプリケーション管理ＡＰを設定するようにしても良い。この場合、クレジット会社から販売元へ購入料金に対応する電子マネー情報を送金する形式やクレジット会社より販売元の銀行口座へ料金を振り込む形式が考えられる。また、上記例に対して、銀行ＡＴＭ用ＡＰと電子決済用ＡＰの処理を並行して処理させ、利用者の振り込み処理のバックグラウンドで電子決済用ＡＰによる販売元への振り込み処理を実行するようにするとなお良い。このようにディジタル映像の再生アプリケーションと異なる別のアプリケーションを使って回収することで、販売元と利用者間の回収ルートが拡張され、販売元への回収のための処理を利用者に意識させずに、より確実で拡張性のある料金回収ルートが確立できる。

【００６７】

以上の実施例における秘密かぎ情報の複製の制御や秘密かぎ情報の複写と共に販売エリアへの金額移動させる制御、販売エリアからセンターへ回収させる制御は、販売元等から配信、提供された秘密かぎ情報制御プログラムに規定されており、この秘密かぎ情報制御プログラムは、秘密かぎ情報の複製と共に、それぞれの利用者カードや、記憶媒体等に記憶される。

【００６８】

本発明の第２の実施例を図１５、図１６を用いて説明する。本実施例は、ディジタル情報とキー情報を複製する際には、キー情報を使用不可の状態で複製させ、センターへアクセスすることにより、キー情報を解除するものである。

図１５に、本実施例のシステム構成を示す。ディジタル情報販売元１５０はディジタル情報を販売するセンター等である。ディジタル情報販売元１５０には、ディジタル情報と、キー情報と、キー情報制御プログラムを含む販売者側プログラムを格納する記憶媒体を有するディジタルデータ販売装置が設置されている。サポートセンタ１５１はディジタル情報の利用に関する操作の説明、最新情報の紹介などを行う。

記憶媒体１５３は、第１の利用者の記憶媒体であり、記憶媒体はハードディスク、光磁気ディスク、磁気ディスク、ＩＣカード、メモリーカード、ＳＩＭカードなど形態はなんでも良い。記憶媒体１５３は、販売元より購入したディジタル情報１５４を記憶する。ディジタル情報１５４は、不正使用を防止するため、暗号化されている。メモリ１５５は、第１の利用者のディジタル情報利用のために必要な情報を格納し、ディジタル情報１５４を使用するためのキー情報１５６を格納する。例えば、キー情報１５６は、暗号化されたディジタル情報１５４を複号化するための秘密かぎ等である。

記憶媒体１５７は、第２の利用者の記憶媒体である。記憶媒体１５７は、第１の利用者の記憶媒体１５３から複製したディジタル情報１５８を記憶する。メモリ１５９は、第２の利用者のディジタル情報利用のために必要な情報を格納する。キー情報１６０は、ロック情報１６１によりロック、つまり使用不可の状態にされる。

【００６９】

この構成において、ディジタル情報１５４はキー情報１５６により利用可能となっている。まず、第１の利用者は、ディジタル情報販売元１５０から、ディジタル情報１５４とキー情報１５６に対する料金を支払うことにより、第１の利用者の記憶媒体１５３にディジタル情報１５４とキー情報１５６及びキー情報制御プログラムを書き込んでもらう。そして、第１の利用者は、ディジタル情報１５４を再生する際に、キー情報１５６を用いて暗号化されたディジタル情報を複号化し、ディジタル情報を再生する構成とする。なお、この複号化は、ディジタル情報の再生する毎に行うものとする。以上の動作は、第1の実施例において説明したものと同様であり、図１おいて説明したディジタル情報販売装置１及びディジタル情報制御装置１３を使用する。

【００７０】

次に、ディジタル情報販売元１から情報を取得した第１の利用者から、第２の利用者へのディジタル情報を複写させる際の方法について説明する。

第１の利用者の記憶媒体１５３から、第２の利用者への記憶媒体１５７のディジタルデータ、キー情報の複製の際には、第1の実施例において説明した、ディ

ジタル情報制御装置１３を使用する。ここで第1の実施例と異なるのは、キー情報の複製方法である。第１の実施例においては、キー情報を使用可能な状態にして、第２の利用者へ複写することとしたが、本実施例においては、第２の利用者へキー情報を複写する場合は、キー情報を使用不可の状態、ロック状態で複写する。なお、ディジタル情報１３４のコピーについては上記で説明した通り、キー情報１３７が利用者の記憶媒体に一緒に存在しないと利用ができないので無制限に複写しても問題がない。また、第1の利用者カード１５３においては、キー情報１５６は、販売元から書き込まれた際、キー情報１３７の状態を示す情報はロック解除状態になっている。キー情報がロック解除状態であるため、第１の利用者は、ディジタル情報１５４を再生できる。

【００７１】

第1の利用者から第2の利用者への複写の手順は以下の通りである。まず、第1の利用者から第2の利用者へディジタル情報の複写の指示を行う。指示が行われると、利用カード制御装置１５、利用者カード制御装置１６を用いて、ディジタル情報１５４と共に、キー情報の複製を行う。このとき、販売元から第1の利用者の記憶媒体に記憶されていたキー情報制御プログラムが、キー情報の複製を制御する。

【００７２】

第１の利用者から第２の利用者へのキー情報１５６の複製の際に、第１の利用者側でロック解除の状態であったキー情報１５６を、ロック状態にして、コピー先の第２の利用者の記憶媒体１５７に書き込む。

【００７３】

ここで、キー情報のロックについて簡単に説明する。キー情報は、１Byteのヘッダー、データサイズを示す１Byteのデータ長、最大２４９Byteの商品名と４Byteの商品コードと１Byteのキー情報のロック状態を示すデータからなる最大２５４Byteのデータ、そして、ヘキサコード１Byteのチェックサムにより構成されるデータである。そして、複写元となる第１利用者の記憶媒体（カード内）に存在するキー情報制御プログラムは上記構成をなすキー情報に対して上記“ロック状態を示すデータ１Byte”の値を変更したキー情報を第２利用者の記憶媒体へ複写

するために生成する。例えば上記ロック状態を示すデータがロック解除の状態を意味する０の値となっている場合、この値をロック状態であることを意味する１の値に設定したキー情報を生成する。また、ロック状態の種別としては“ロック”、“ロック解除”の２つの状態の他にディジタル情報を１０％利用可能であるロック状態を意味する２の値としたり、８０％の利用が可能であるロック状態を意味する３の値としたりすることで、“ロックの状態”に複数の利用範囲を規定することも可能である。上記ロック状態に設定されたキー情報はディジタル情報制御装置の利用者ユニット制御手段２２が利用者カード制御装置１（１５）を制御して第一利用者の記憶媒体（ICカード内臓メモリ）より取得する。

【００７４】

続いて第２利用者の記憶媒体に上記ロック状態に設定されたキー情報を複写（書き込み）するのはディジタル情報制御装置の利用者ユニット制御手段２２が利用者カード制御装置２（１６）を制御して第2利用者の記憶媒体（ICカード内臓のメモリ）へ上記キー情報を複写（書き込む）する。第１利用者記憶媒体及び第２利用者記憶媒体と利用者ユニット制御手段１及び利用者制御ユニット２との関係（装着、はめ込む）はどちらであってもよい。上記のようなロック状態を示すデータの変更を施したキー情報の生成はICカード内部で行うことで高い安全性を得られる。また、キー情報に対して上記キー情報管理プログラムで暗号化処理を施すことでより一層の安全性が得られる。

【００７５】

なお、キー情報の記憶媒体への書き込みには必ず販売元固有のコードを利用し、このコードを利用しないで書き込みを行うと、キー情報１３７にロック情報１３８が必ず付加された形態で記憶媒体に書き込まれる方式を採用することにより、第１の利用者から第２の利用者にキー情報を複製させる場合にロックさせることが可能となる。

【００７６】

第２の利用者は、第１の利用者から複写したディジタル情報１５８を再生しようとしてもキー情報１６０にロック情報１６１が付加されているため、そのまま再生することはできない。ここで、第２の利用者がディジタル情報１５８を再生

するためにはディジタル情報販売元１５０又はサポートセンタ１５１へのアクセスが必要とする。

【００７７】

図１６のフローチャートを用いて、第２の利用者が料金を支払い、ディジタル情報１５７を再生する方法について説明する。

【００７８】

利用者カード制御装置１（カードスロットなど）に先に複写したロック状態のキー情報が格納される第2利用者の記憶媒体（ICカードなど）が装着されると、ディジタル情報制御装置１３の利用者ユニット制御手段（PCなど）の制御により利用者カード制御装置１経由でキー情報を取得する。このキー情報のサポートセンターへの送信は利用者外部通信手段２３（モデムなど）により回線（電話回線など）を経由して行う。

【００７９】

サポートセンターでは受信したキー情報が同センターでサポート可能であるかを判別した後、可能であれば、キー情報より取得した料金を請求することを示す情報を上記回線経由で送信する。次に第2利用者側では請求された金額情報をサポートセンターへ送金する。この金額情報をサポートセンターで受け取った後、受領を意味する領収情報を送信する。続いてサポートセンターでは先に受信した第2利用者からのロック状態のキー情報に対してロックを解除する処理を行う。このロック解除ではディジタル情報の販売元固有のコードによりキー情報の値を演算することが唯一ロック状態を示すデータを変更できるアルゴリズムとなっている。ロック解除の処理が完了するとキー情報をサポートセンター側から第２利用者側へ送信する。また、回線経由で送信されるキー情報には暗号化処理が施されているため、キー情報送信に使用する回線上で同キー情報が盗聴して使用を試みてもそのままの使用はできないことになっている。上記の手順で料金の支払いとロック状態を解除されたキー情報を受信した第２利用者はこのキー情報によりディジタル情報を再生する。

【００８０】

次に、図１７のフローチャートを用いて、第２の利用者が料金を支払い、ディ

ジタル情報１５７を再生する他の方法について説明する。

図１７のフローチャートは、図１６のフローチャートと、サポートセンターで行うキー情報に対しロック解除の処理と料金徴収処理の順番が異なる。

【００８１】

第２次利用者がサポートセンターにアクセスし、キー情報を送信する。キー情報を受信したサポートセンタは、キー情報を判別し、キー情報のロック解除を開始する。ロック解除が完了した後、請求情報を転送する。

【００８２】

第２次利用者が代金を送金し、決済が完了すると、サポートセンタが涼秋情報と、ロック解除のためのキー情報を送信する。

【００８３】

図１６と図１７では、ロック解除の処理と料金徴収処理の順番が異なるために、エラー発生またはロック解除キャンセル時の処理が異なる。図１６ではキー情報のロック解除処理を代金受領の後に行うため、利用者の要求でロック解除キャンセルとなった場合にロック解除処理を行わずに済むため、サポートセンターとしては不要な処理が発生しない形態となる。図１７では、前もってロック解除の処理を行うことで、代金受領後に処理したキー情報を素早く送信できるため、利用者の待ち時間が減少する。また、代金受領後の回線切断により利用者へキー情報を送信できない確率が低くなる。

【００８４】

なお、支払は現金決済でも良いし、電子マネー決済でも良い。また、キー情報はディジタル情報個々に異なるものなので、複数のディジタル情報を利用する場合、各キー情報に対して販売元エリアの電子マネーを個別に格納すると購入料金回収先となる販売元を区別したり、振り込みなどの処理を行う際、利便性が向上する。

【００８５】

さらに、複数のキー情報を格納することで、上記キー情報１３７を格納するメモリの容量が不足した場合、その旨を利用者に通知して、不必要なキー情報を消去できるようにしても良い。また、上記複写の開始時に、“複写は有料”である

ことを利用者へ知らせることは必要なガイダンスの１つであり、通知の形態は問わないが必ず行う。

【００８６】

また、図示しないがサポートセンタ１３１に支払われた利用者からの購入料金はオンラインでリアルタイムにディジタル情報販売元１３０へ送金することにしても良い。

【００８７】

方法により第３、第４とディジタル情報のコピーが利用者間で行われても、コピー実行時には販売元が回収可能な金額情報が生成され、再生時の利用者のアクセスにより、必ず販売元へディジタル情報に対する購入料金が回収できることになり、利用者間における複製行動を利用した拡販が期待できるため、販売者と利用者の直接販売と異なる形態（利用者間の口コミ販売のようなもの）には、効果的な方法となる。

【００８８】

本実施例においては、ディジタル情報１５４、１５８と、キー情報１５６、１６０を同じ記憶媒体１５３、１５７に記憶させる例を説明したが、第１の実施例と同様に、別々の媒体に記憶させてもよい。また、第１の実施例と同様に、キー情報を利用者固有の秘密かぎ情報により暗号化することにより、利用者情報に関連した暗号化情報を利用してこととなるので、利用者間の複製に対して安全性の高いディジタル情報の販売システムとなる。なお、本実施例におけるキー情報の複製の制御やキー情報のロック解除制御は、販売元等から配信、提供されたキー情報制御プログラムに規定されており、このキー情報制御プログラムは、キー情報の複製と共に、それぞれの利用者記憶媒体等に記憶される。

【００８９】

なお、キー情報を使用不可の状態で複製させる本実施例は、第２の利用者へのキー情報複製を禁止する構成と比べて、セキュリティを高くすることができる。例えば、第２の利用者へのキー情報複製を禁止し、キー情報をアクセスにより手に入れる方法では、１種類のディジタル情報（例えば、ある映画１本、ある音楽１曲）については、同じ１つのキー情報を使用しなくてはならない。このような

方式では、あるキー情報が解読されてしまうと、多数の人間がそのディジタル情報を複合化して使用できるため、セキュリティが低くなってしまう。キー情報を使用不可の状態で複製させる本実施例においては、１種類のディジタル情報について、複数のキー情報を割り当てることができる。複数のキー情報を割り当てても、複製されたキー情報をサポートセンターに送信することにより、キー情報をセンターで照会できるからである。従って、１種類のディジタル情報（例えば、ある映画１本、ある音楽１曲）に複数のキー情報を割り当てた場合は、１つのキー情報が解読されたからといって、その他のキー情報を持つディジタル情報は使用できないため、セキュリティを高くすることができる。

【００９０】

以上のように本実施例では、利用者間で複製されたディジタル情報の利用時には、必ず利用者による販売元へのアクセスを必要とする方式としているので、販売元は確実にディジタル情報の利用に対する料金を回収できることになる。この方式によれば、ネットワークに接続された再生端末を所有する利用者間のディジタル情報の複製を管理可能であり、利用者からの要求によりリアルタイムでディジタル情報の利用を許可にしたり、また、その料金を回収することができることとなる。

【００９１】

【発明の効果】

本発明によれば、ディジタル情報の販売、配信に際して、利用者間の不正な複製を防止でき、料金を回収できるという効果が得られる。

【図面の簡単な説明】

【図１】

本発明の一実施例のシステム構成１を示す図である。

【図２】

本発明の一実施例のディジタル情報販売手順を示すフローチャートである。

【図３】

本発明の一実施例のディジタル情報再生手順を示すフローチャートである。

【図４】

本発明の一実施例のディジタル情報転売手順を示すフローチャートである。

【図５】

本発明の一実施例のＩＣカードの構成１を示す図である。

【図６】

本発明の一実施例の利用者間を移動する情報の流れを示す図である。

【図７】

本発明の一実施例の利用者間の料金回収手順１を示すフローチャートである。

【図８】

本発明の一実施例のシステムの構成２を示す図である。

【図９】

本発明の一実施例のＩＣカードの構成２を示す図である。

【図１０】

本発明の一実施例の利用者間の料金回収手順２を示すフローチャートである。

【図１１】

本発明の一実施例の利用者間の料金回収手順３を示すフローチャートである。

【図１２】

本発明の一実施例のシステムの構成を示す図である。

【図１３】

本発明の一実施例の銀行ＡＴＭの回収手順１を示すフローチャートである。

【図１４】

本発明の一実施例の銀行ＡＴＭの回収手順２を示すフローチャートである。

【図１５】

本発明の一実施例のシステムの構成を示す図である。

【図１６】

本発明の一実施例の料金の回収手順を示すフローチャートである。

【図１７】

本発明の一実施例の料金の回収手順を示すフローチャートである。

【符号の説明】

１	ディジタル情報販売装置
２	ディジタル情報
３	暗号化情報生成器
４	販売元所有のＩＣカード
５	販売元所有ＩＣカード制御装置
６	利用者所有のＩＣカード
６－１	第１利用者のＩＣカード
６－２	第２利用者のＩＣカード
７	利用者所有ＩＣカード制御装置
８	販売履歴メモリ
９	販売社外部通信手段
１０	販売元プログラム格納メモリ
１１	販売者側外部入出力手段
１２	販売者ユニット制御手段
１３	ディジタル情報制御装置
１４	暗号化情報再生器
１５	利用者カード制御装置１
１６	利用者カード制御装置２
１７	ディジタル情報格納媒体制御装置
１８	利用者側プログラム格納メモリ
１９	利用者側プログラム制御手段
２０	ディジタル情報再生手段
２１	利用者側入出力手段
２２	利用者ユニット制御手段
２３	利用者側外部通信手段
３０	Ｉ／Ｏ（ＩＣカードインタフェース信号入出力部）
３１	履歴格納メモリ
３２	暗号／復号化手段

３３　メモリ
３４　キー管理メモリ
３４－１　第１利用者キー情報格納エリア
３４－２　販売者キー格納情報エリア
３５　ロック管理メモリ
３５－１　第１利用者ロック情報格納エリア
３６　電子マネー格納メモリ
３６－１　第１利用者専用エリア
３６－２　販売元専用エリア
３８　演算手段
３９　アクセス管理手段
４０　Ｉ／Ｏ（ＩＣカードインタフェース信号入出力部）
４１　履歴格納メモリ
４２　暗号／復号化手段
４３　メモリ
４４　キー管理メモリ
４４－１　第２利用者キー情報格納エリア
４４－２　販売者キー格納情報エリア
４５　ロック管理メモリ
４５－１　第２利用者ロック情報格納エリア
４６　電子マネー格納メモリ
４６－１　第２利用者専用エリア
４６－２　販売元専用エリア
４８　演算手段
４９　アクセス管理手段
５０　ディジタル情報販売店
５１　ディジタル情報
５２　販売元固有の暗号化情報
５３　販売元固有の秘密かぎ情報

５４　販売者所有のＩＣカード

５５　暗号化されたディジタル情報

６０　第１利用者オンライン端末

６１　第１利用者固有の秘密かぎ情報

６２　第１利用者固有の暗号化情報

６３　第１利用者のＩＣカード

６４　第１利用者固有の暗号化情報で暗号化された販売元固有の秘密かぎ情報

７０　第２利用者オフライン端末

７１　第２利用者固有の秘密かぎ情報

７２　第２利用者固有の暗号化情報

７３　第２利用者のＩＣカード

７４　第２利用者固有の暗号化情報で暗号化された販売元固有の秘密かぎ情報

８０　第３利用者オフライン端末

８１　第３利用者固有の秘密かぎ情報

８２　第３利用者固有の暗号化情報

８３　第３利用者のＩＣカード

８４　第３利用者固有の暗号化情報で暗号化された販売元固有の秘密かぎ情報

９０　第Ｎ利用者オンライン端末

９１　第Ｎ利用者固有の秘密かぎ情報

９２　第Ｎ利用者固有の暗号化情報

９３　第Ｎ利用者のＩＣカード

９４　第Ｎ利用者固有の暗号化情報で暗号化された販売元固有の秘密かぎ情報

１００　販売元

１０１　第１利用者オンライン環境下の端末

１０２　第２利用者オフライン環境下の端末

１０３　第３利用者オフライン環境下の端末
１０４　第４利用者オンライン環境下の端末
１０５　第５利用者オフライン環境下の端末
１０６　第６利用者オフライン環境下の端末
１０７　第７利用者オフライン環境下の端末
１０８　第８利用者オンライン環境下の端末
１０９　第ｎ利用者オンライン環境下の端末
１１０　回線
１２０　演算手段
１２１　Ｉ／Ｏ（ＩＣカードインタフェース信号入出力部）
１２２　暗号／復号化手段
１２３　制御プログラム格納メモリ
１２４　プロバイダ契約情報格納メモリ
１２５　履歴格納メモリ
１２６　電子マネー格納メモリ
１２６－１　第１利用者専用エリア
１２６－２　販売元専用エリア
１２７　アクセス管理手段
１２８　ロック管理メモリ
１２８－１　第１利用者ロック情報格納エリア
１２９　キー管理メモリ
１２９－１　第２利用者キー情報格納エリア
１２９－２　販売者キー格納情報エリア
１４０　ディジタル映像販売元
１４１　銀行ＡＴＭ
１４２　利用者１の金額情報格納エリア
１４２－１　利用者１の利用者専用エリア
１４２－２　利用者１の販売元専用エリア
１４３　利用者１のアプリケーション格納メモリ

１４４　　キー管理メモリ

１４５　　ディジタル映像情報

１４６　　利用者２のアプリケーション格納メモリ

１４７　　利用者２の金額情報格納エリア

１４７－１　利用者２の利用者専用エリア

１４７－２　利用者２の販売元専用エリア

１５０　　ディジタル情報提供元

１５１　　サポートセンタ

１５３　　第１の利用者の記憶媒体

１５７　　第２の利用者２の記憶媒体

１６０　　ディジタル情報利用のためのキー情報

１６１　　ディジタル情報利用のためのキー情報のロック情報

【書類名】　図面

【図１】

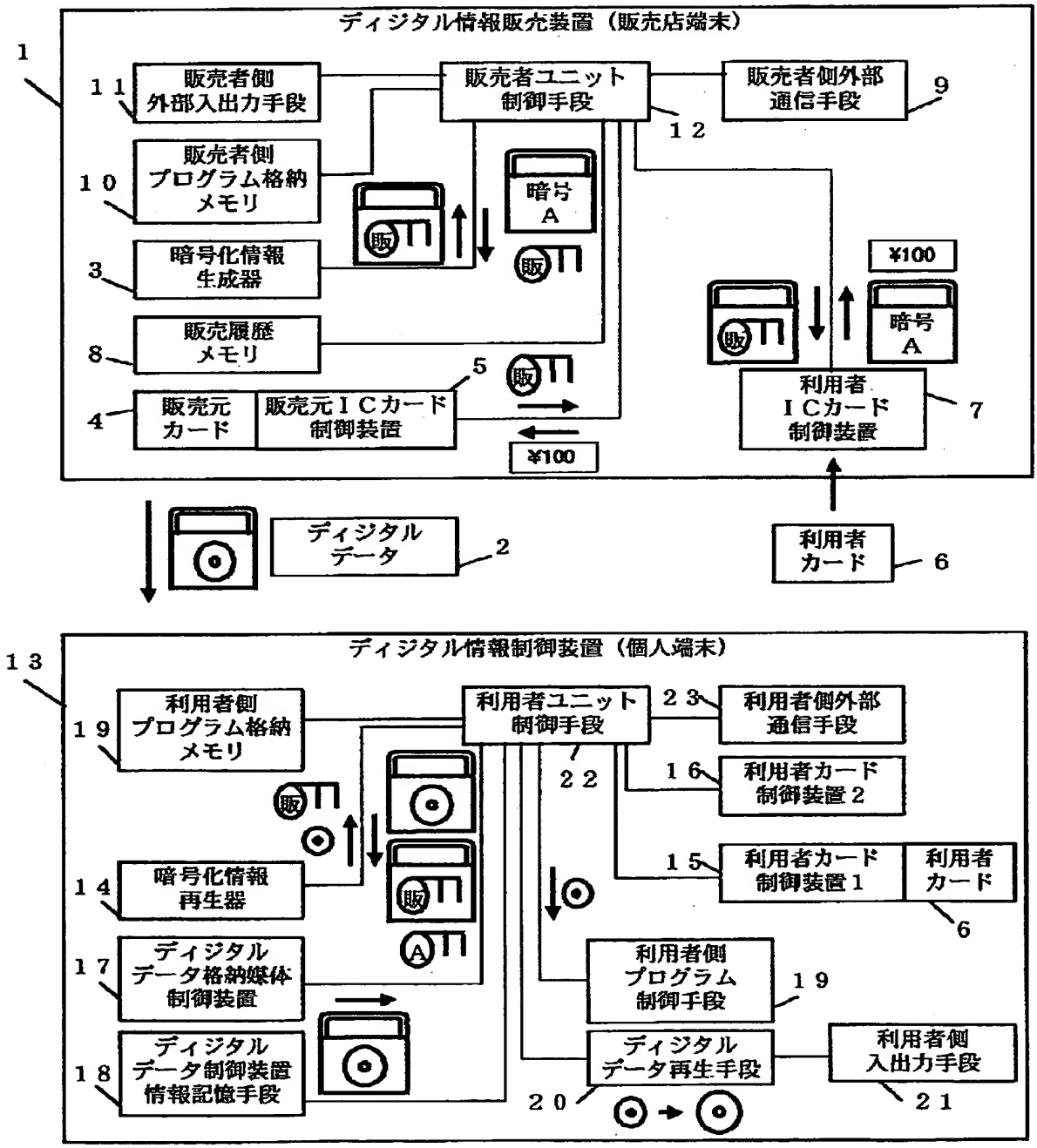

図１

出証特２０００－３１０６２３９

【図２】

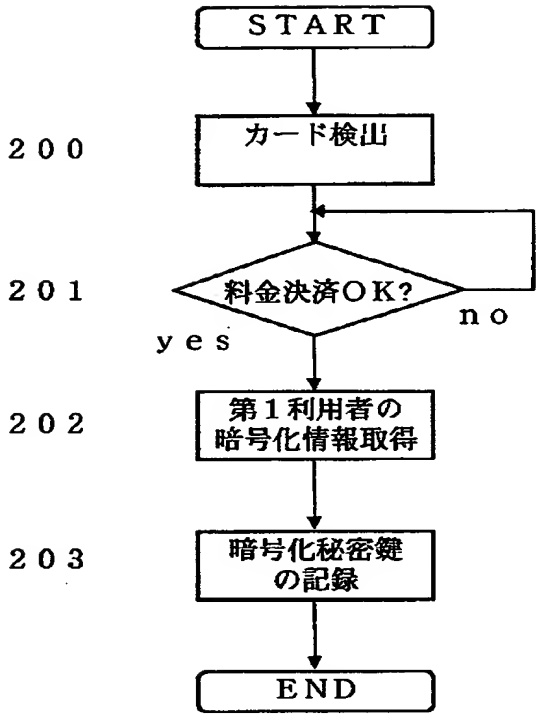
START
２００
カード検出
２０１
料金決済ＯＫ?
no
ｙｅｓ
２０２
第１利用者の
暗号化情報取得
２０３
暗号化秘密鍵
の記録
END

図２

【図３】

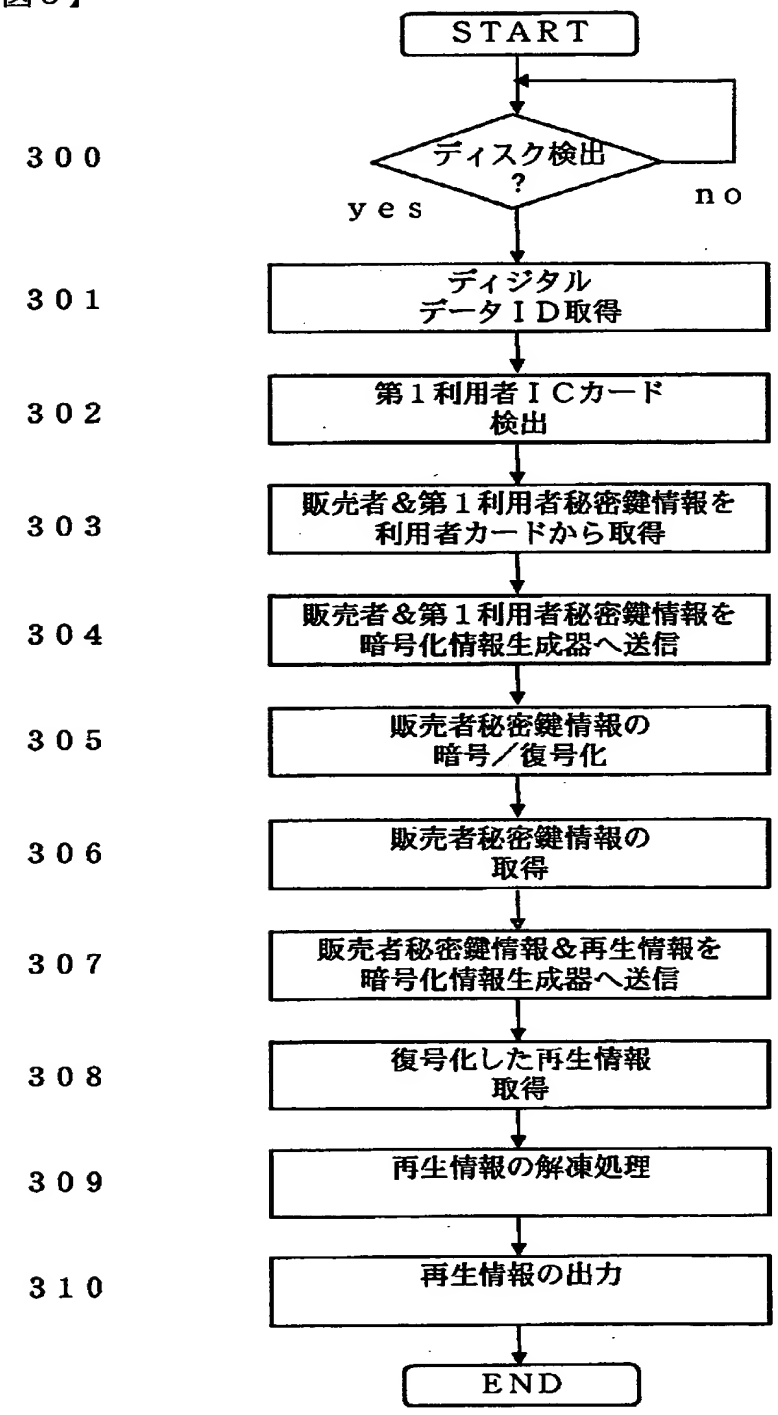

図３

出証特２０００－３１０６２３９

【図４】

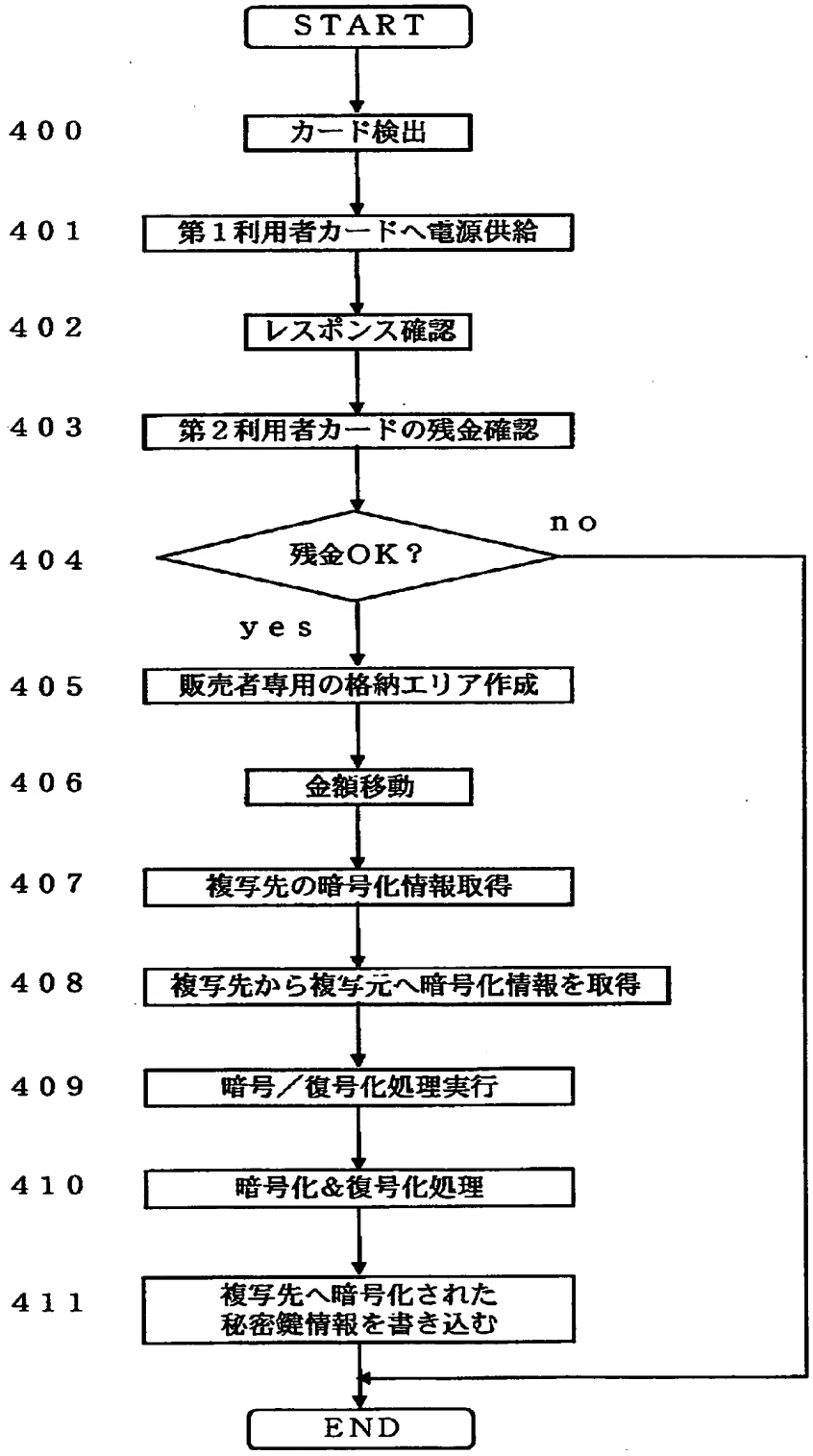
START
４００
カード検出
４０１
第１利用者カードへ電源供給
４０２
レスポンス確認
４０３
第２利用者カードの残金確認
４０４
残金ＯＫ？
ｎｏ
ｙｅｓ
４０５
販売者専用の格納エリア作成
４０６
金額移動
４０７
複写先の暗号化情報取得
４０８
複写先から複写元へ暗号化情報を取得
４０９
暗号／復号化処理実行
４１０
暗号化＆復号化処理
４１１
複写先へ暗号化された
秘密鍵情報を書き込む
END

図４

【図５】

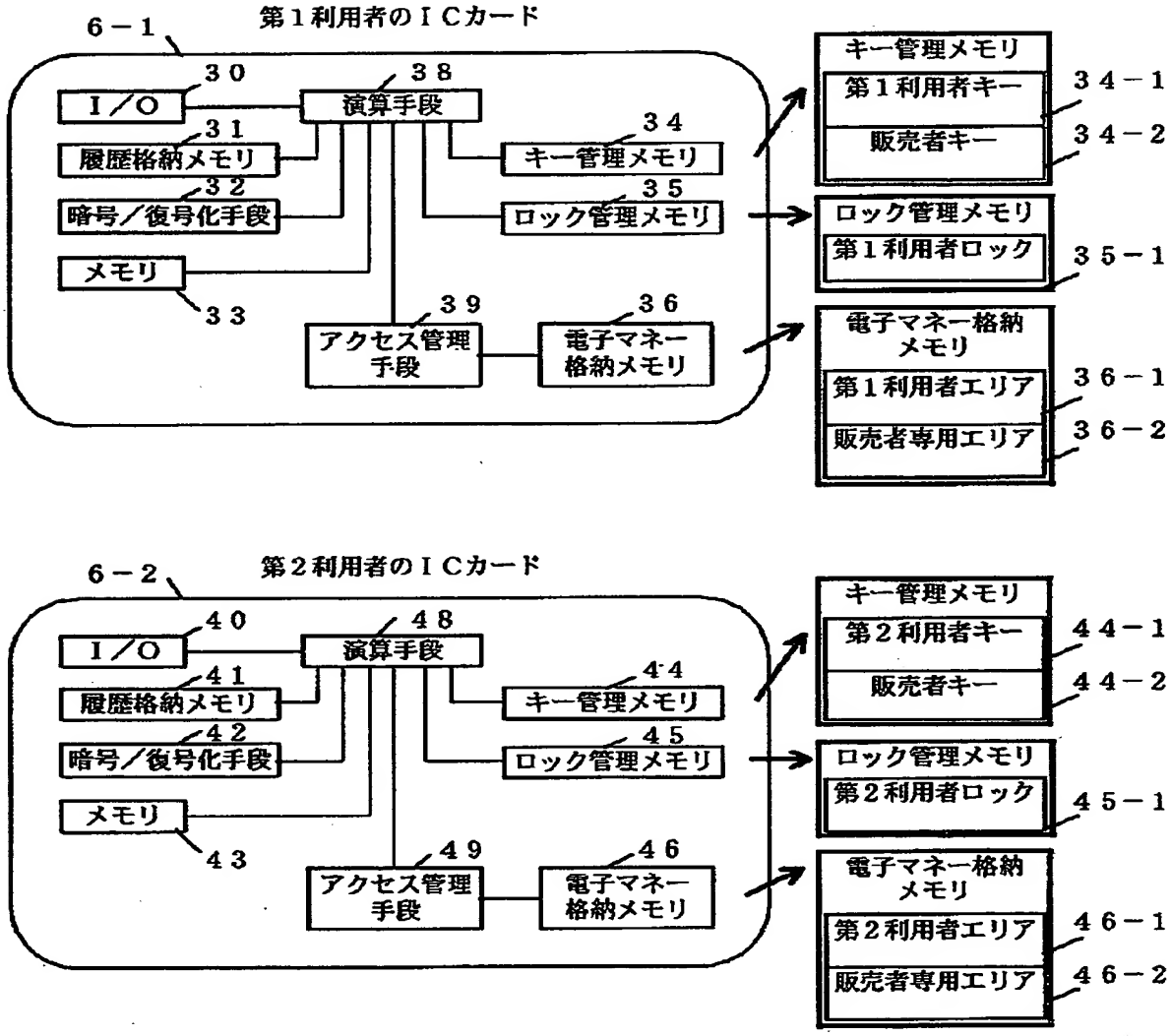
6－1
第１利用者のＩＣカード
３０
３８
Ｉ／Ｏ
演算手段
３１
履歴格納メモリ
３４
キー管理メモリ
３２
暗号／復号化手段
３５
ロック管理メモリ
メモリ
３３
３９
３６
アクセス管理手段
電子マネー格納メモリ
キー管理メモリ
第１利用者キー
３４－１
販売者キー
３４－２
ロック管理メモリ
第１利用者ロック
３５－１
電子マネー格納メモリ
第１利用者エリア
３６－１
販売者専用エリア
３６－２
6－2
第２利用者のＩＣカード
４０
４８
Ｉ／Ｏ
演算手段
４１
履歴格納メモリ
４４
キー管理メモリ
４２
暗号／復号化手段
４５
ロック管理メモリ
メモリ
４３
４９
４６
アクセス管理手段
電子マネー格納メモリ
キー管理メモリ
第２利用者キー
４４－１
販売者キー
４４－２
ロック管理メモリ
第２利用者ロック
４５－１
電子マネー格納メモリ
第２利用者エリア
４６－１
販売者専用エリア
４６－２

図５

【図６】

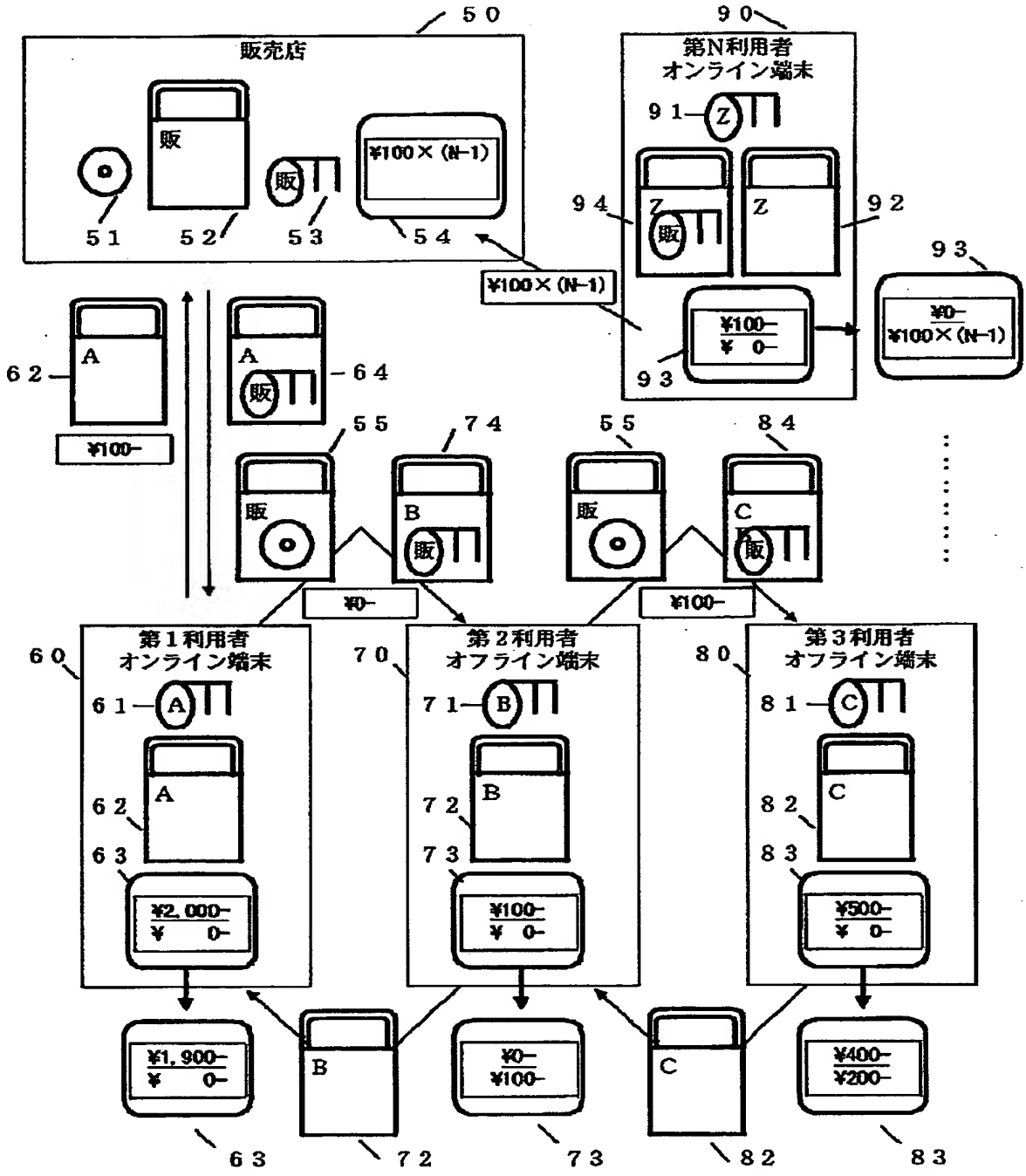
５０
販売店
販
販
¥100×(N-1)
５１
５２
５３
５４
９０
第N利用者
オンライン端末
９１
Z
９４
Z
販
Z
９２
９３
¥100－
¥ 0－
¥0－
¥100×(N-1)
¥100×(N-1)
６２
A
¥100－
A
販
６４
５５
７４
５５
８４
販
B
販
販
C
販
¥0－
¥100－
６０
第１利用者
オンライン端末
６１
A
６２
６３
¥2,000－
¥ 0－
７０
第２利用者
オフライン端末
７１
B
７２
７３
¥100－
¥ 0－
８０
第３利用者
オフライン端末
８１
C
８２
８３
¥500－
¥ 0－
¥1,900－
¥ 0－
B
¥0－
¥100－
C
¥400－
¥200－
６３
７２
７３
８２
８３

図６

【図７】

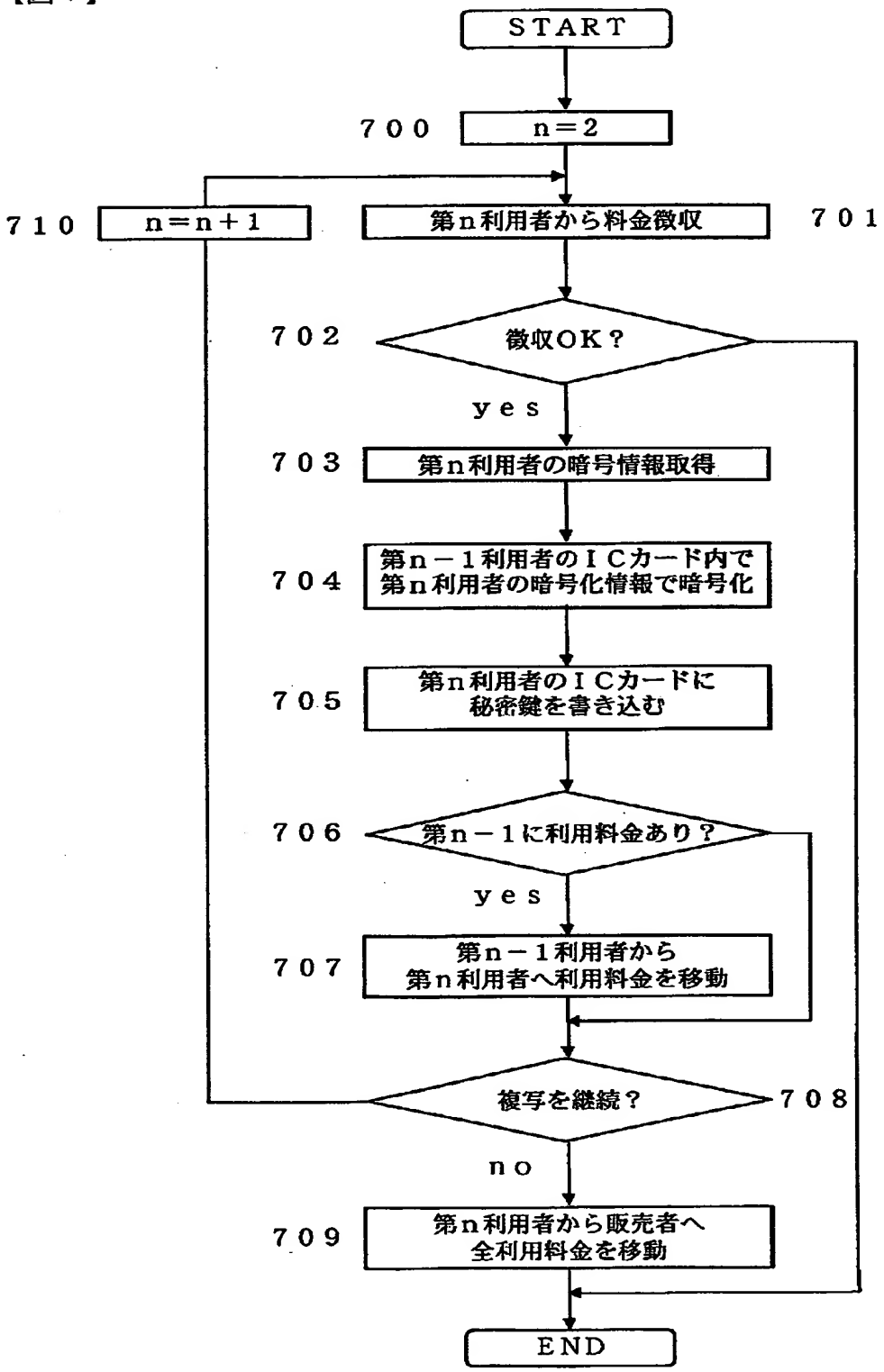
START
７００
n＝2
７１０
n＝n＋1
第ｎ利用者から料金徴収
７０１
７０２
徴収OK？
ｙｅｓ
７０３
第ｎ利用者の暗号情報取得
７０４
第ｎ－１利用者のＩＣカード内で
第ｎ利用者の暗号化情報で暗号化
７０５
第ｎ利用者のＩＣカードに
秘密鍵を書き込む
７０６
第ｎ－１に利用料金あり？
ｙｅｓ
７０７
第ｎ－１利用者から
第ｎ利用者へ利用料金を移動
複写を継続？
７０８
ｎｏ
７０９
第ｎ利用者から販売者へ
全利用料金を移動
END

図７

【図８】

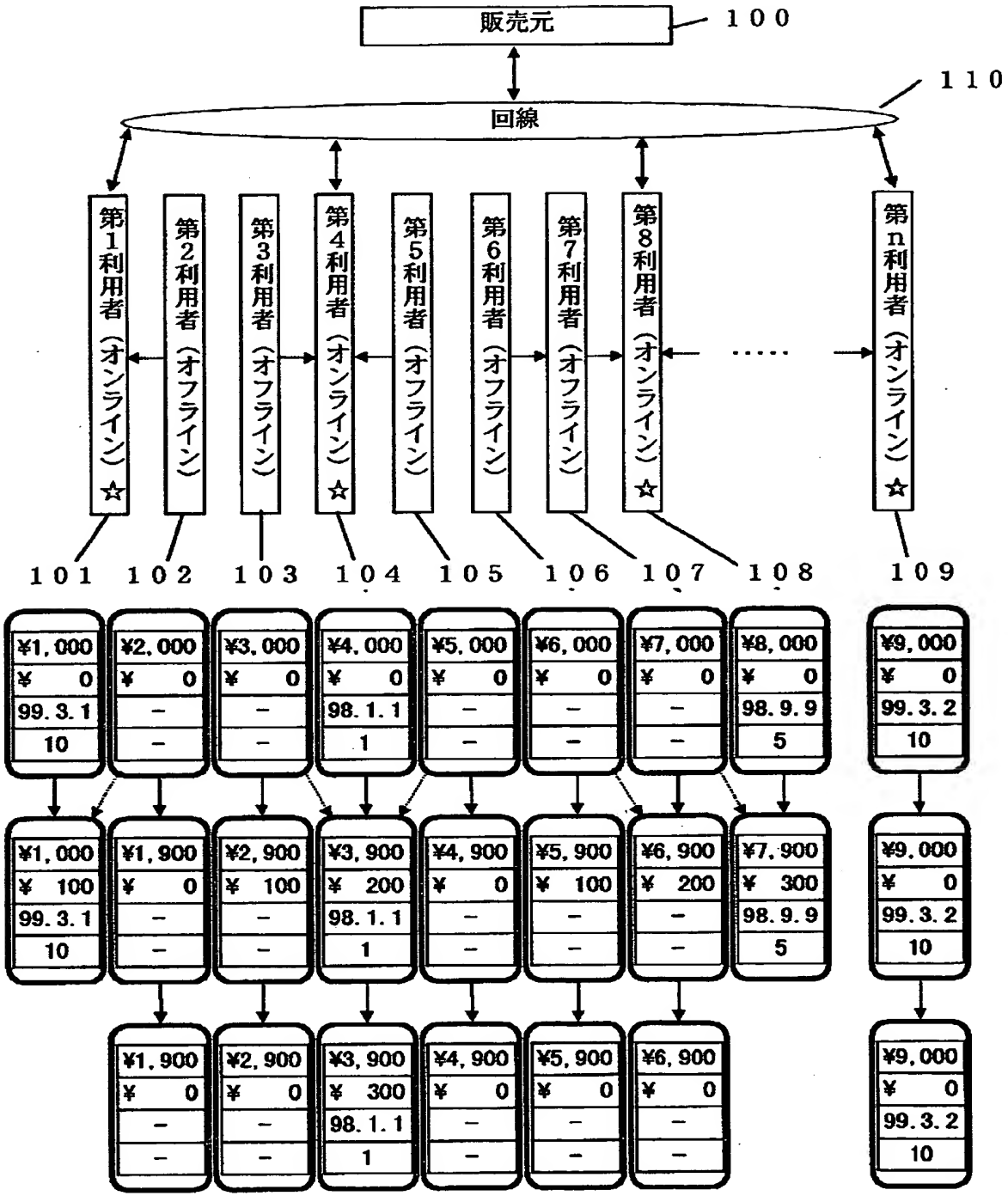
販売元
１００
１１０
回線
第1利用者（オンライン）☆
第2利用者（オフライン）
第3利用者（オフライン）
第4利用者（オンライン）☆
第5利用者（オフライン）
第6利用者（オフライン）
第7利用者（オフライン）
第8利用者（オンライン）☆
第n利用者（オンライン）☆
１０１ １０２ １０３ １０４ １０５ １０６ １０７ １０８ １０９
¥1,000 ¥ 0 99.3.1 10
¥2,000 ¥ 0 – –
¥3,000 ¥ 0 – –
¥4,000 ¥ 0 98.1.1 1
¥5,000 ¥ 0 – –
¥6,000 ¥ 0 – –
¥7,000 ¥ 0 – –
¥8,000 ¥ 0 98.9.9 5
¥9,000 ¥ 0 99.3.2 10
¥1,000 ¥ 100 99.3.1 10
¥1,900 ¥ 0 – –
¥2,900 ¥ 100 – –
¥3,900 ¥ 200 98.1.1 1
¥4,900 ¥ 0 – –
¥5,900 ¥ 100 – –
¥6,900 ¥ 200 – –
¥7,900 ¥ 300 98.9.9 5
¥9,000 ¥ 0 99.3.2 10
¥1,900 ¥ 0 – –
¥2,900 ¥ 0 – –
¥3,900 ¥ 300 98.1.1 1
¥4,900 ¥ 0 – –
¥5,900 ¥ 0 – –
¥6,900 ¥ 0 – –
¥9,000 ¥ 0 99.3.2 10

図８

【図９】

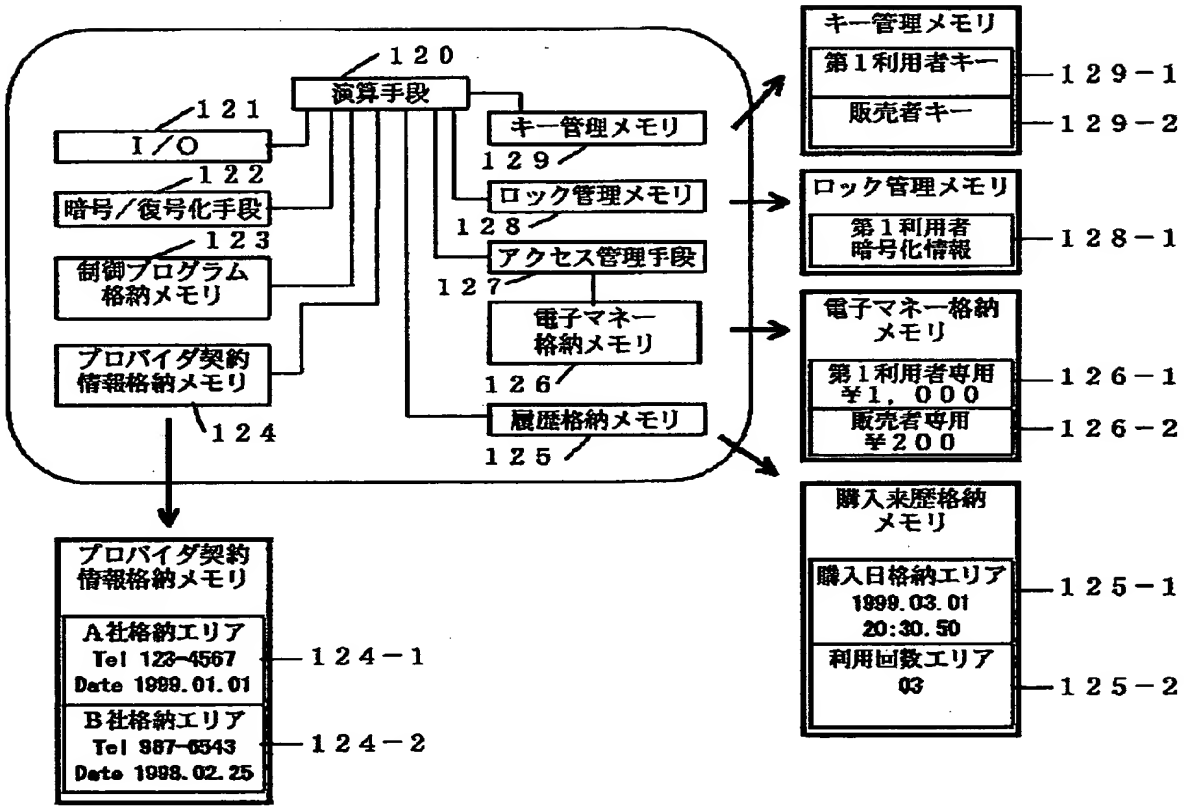
１２０
演算手段
１２１
Ｉ／Ｏ
１２２
暗号／復号化手段
１２３
制御プログラム格納メモリ
プロバイダ契約情報格納メモリ
１２４
キー管理メモリ
１２９
ロック管理メモリ
１２８
アクセス管理手段
１２７
電子マネー格納メモリ
１２６
履歴格納メモリ
１２５
キー管理メモリ
第１利用者キー
販売者キー
１２９－１
１２９－２
ロック管理メモリ
第１利用者暗号化情報
１２８－１
電子マネー格納メモリ
第１利用者専用 ￥１，０００
販売者専用 ￥２００
１２６－１
１２６－２
購入来歴格納メモリ
購入日格納エリア 1999.03.01 20:30.50
利用回数エリア 03
１２５－１
１２５－２
プロバイダ契約情報格納メモリ
Ａ社格納エリア Tel 123-4567 Date 1999.01.01
Ｂ社格納エリア Tel 987-6543 Date 1998.02.25
１２４－１
１２４－２

図９

【図１０】

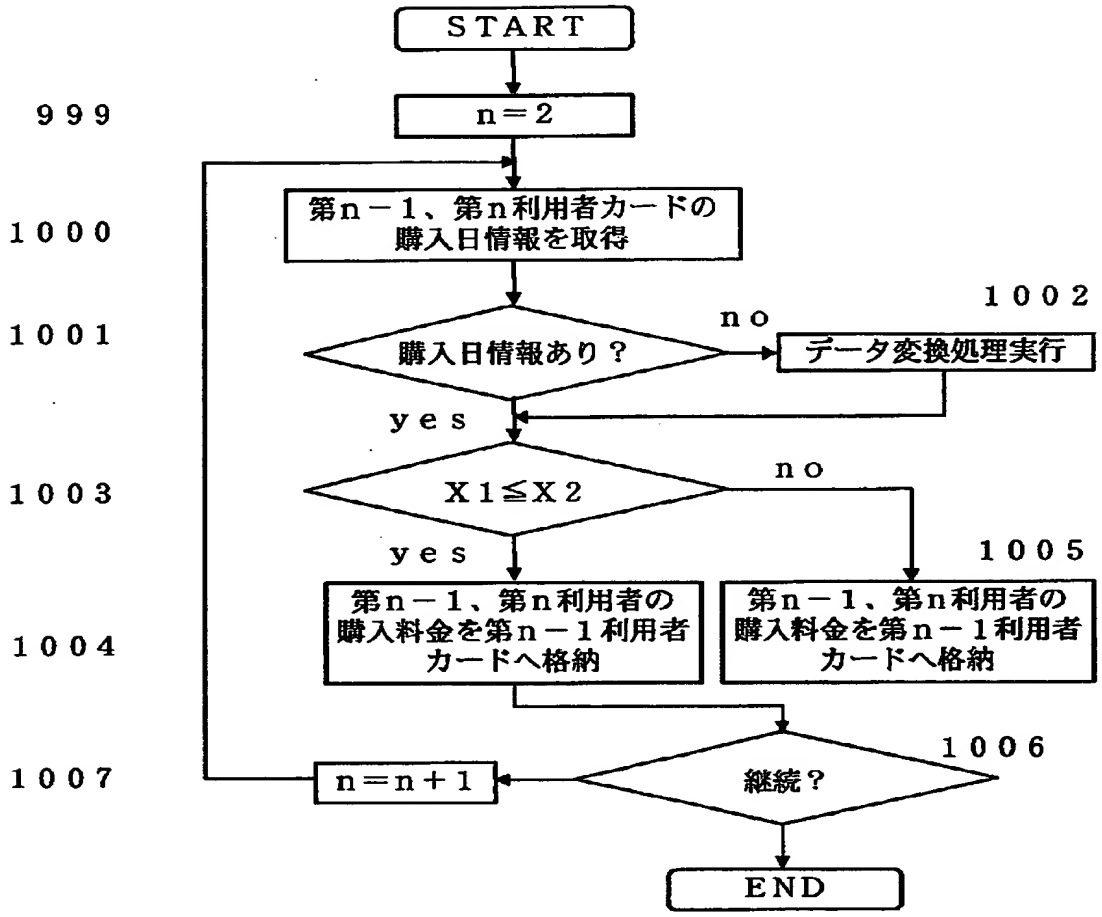
START
999
n＝2
1000
第ｎ－１、第ｎ利用者カードの購入日情報を取得
1001
購入日情報あり？
no
1002
データ変換処理実行
yes
1003
X1≦X2
no
1005
yes
1004
第ｎ－１、第ｎ利用者の購入料金を第ｎ－１利用者カードへ格納
第ｎ－１、第ｎ利用者の購入料金を第ｎ－１利用者カードへ格納
1006
継続？
1007
n＝n＋1
END

図１０

【図１１】

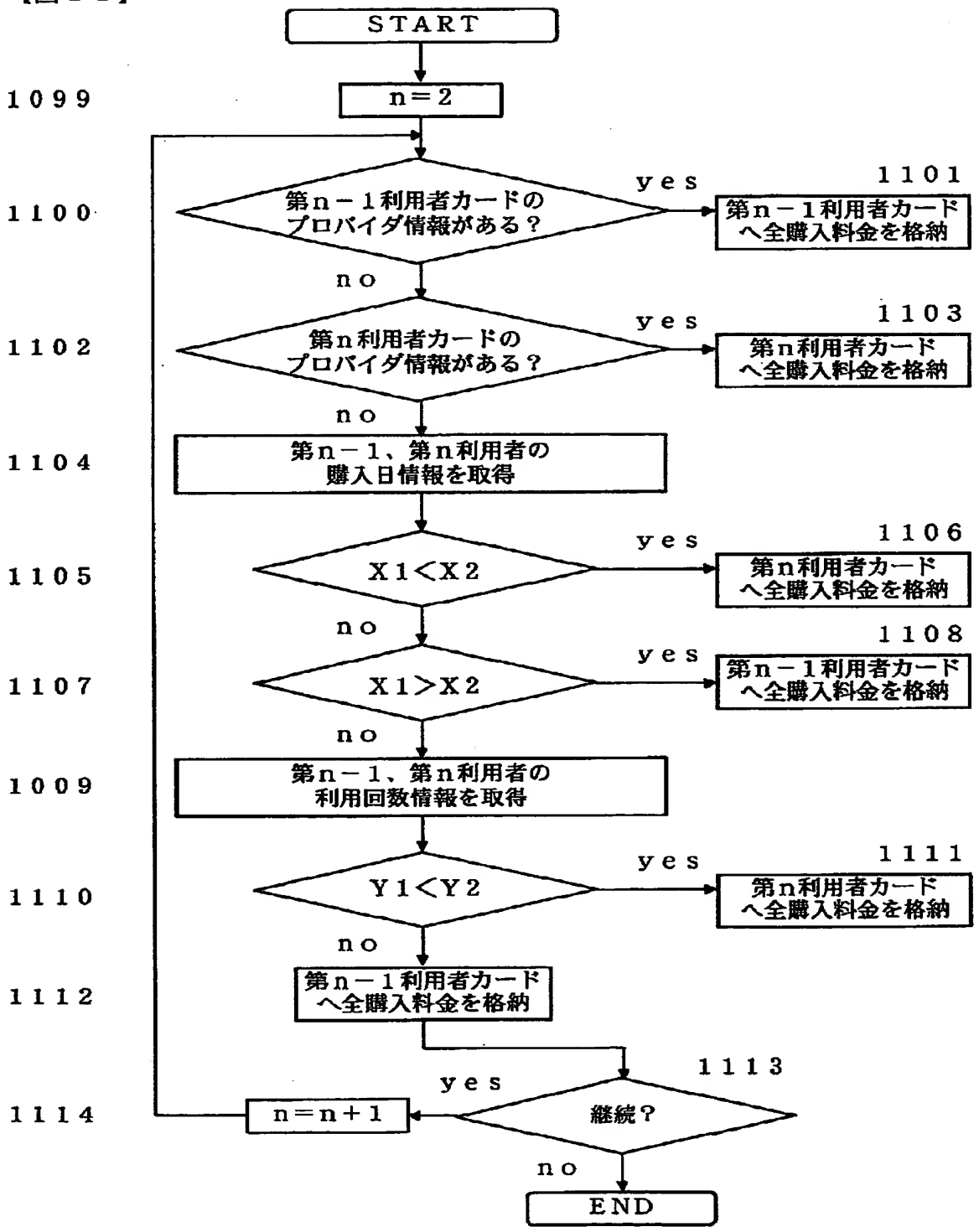

図１１

出証特２０００－３１０６２３９

【図１２】

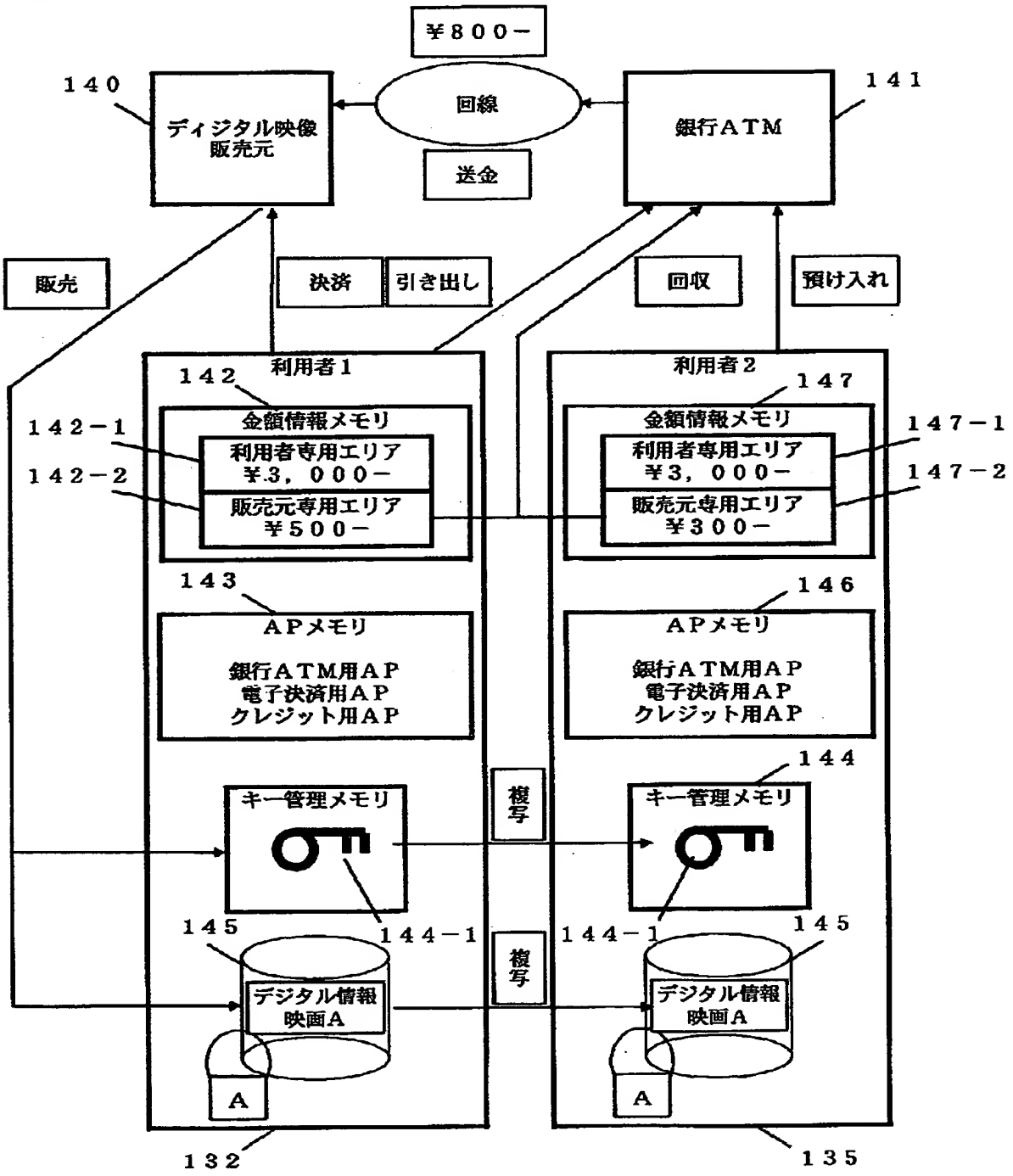
￥８００－
１４０
ディジタル映像
販売元
回線
送金
銀行ＡＴＭ
１４１
販売
決済
引き出し
回収
預け入れ
利用者１
１４２
金額情報メモリ
１４２－１
利用者専用エリア
￥３，０００－
１４２－２
販売元専用エリア
￥５００－
１４３
ＡＰメモリ
銀行ＡＴＭ用ＡＰ
電子決済用ＡＰ
クレジット用ＡＰ
キー管理メモリ
１４４－１
１４５
デジタル情報
映画Ａ
Ａ
１３２
利用者２
１４７
金額情報メモリ
１４７－１
利用者専用エリア
￥３，０００－
１４７－２
販売元専用エリア
￥３００－
１４６
ＡＰメモリ
銀行ＡＴＭ用ＡＰ
電子決済用ＡＰ
クレジット用ＡＰ
１４４
キー管理メモリ
１４４－１
１４５
デジタル情報
映画Ａ
Ａ
１３５
複写
複写

図１２

【図１３】

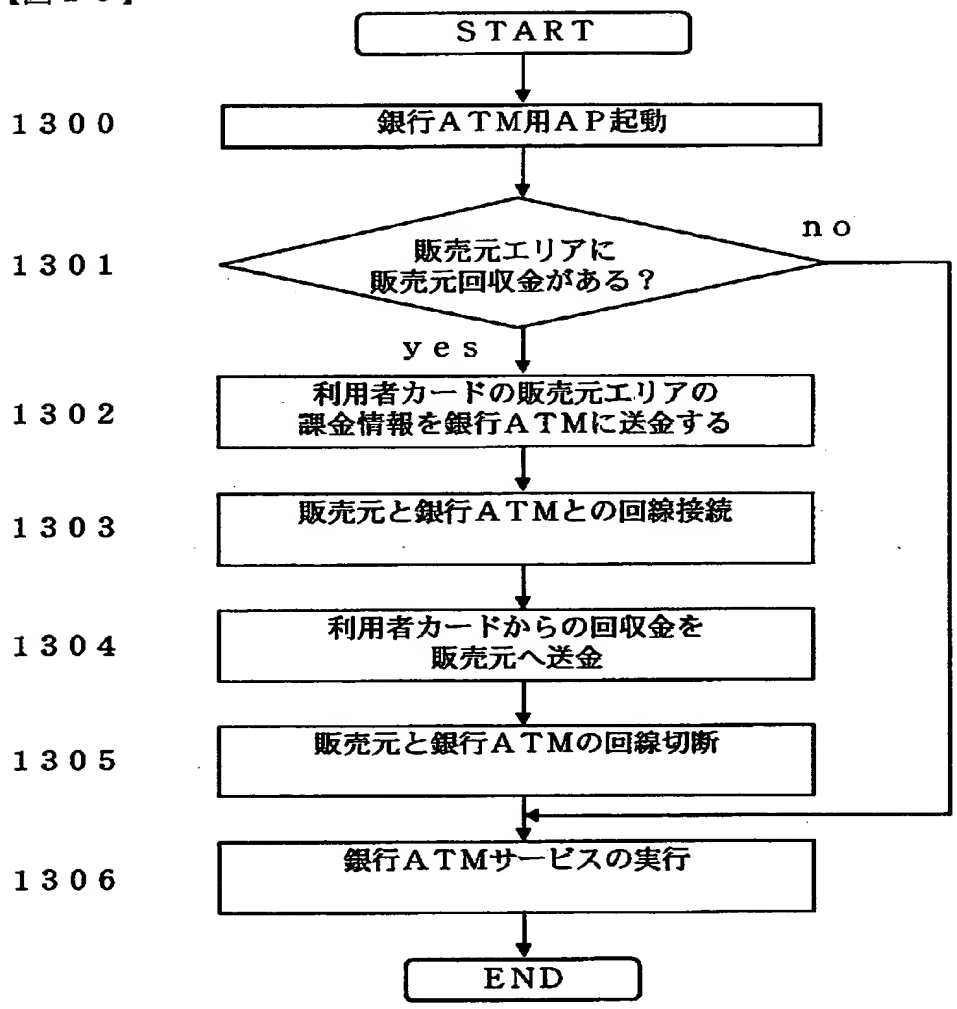
START
１３００
銀行ＡＴＭ用ＡＰ起動
１３０１
販売元エリアに
販売元回収金がある？
ｎｏ
ｙｅｓ
１３０２
利用者カードの販売元エリアの
課金情報を銀行ＡＴＭに送金する
１３０３
販売元と銀行ＡＴＭとの回線接続
１３０４
利用者カードからの回収金を
販売元へ送金
１３０５
販売元と銀行ＡＴＭの回線切断
１３０６
銀行ＡＴＭサービスの実行
END

図１３

【図１４】

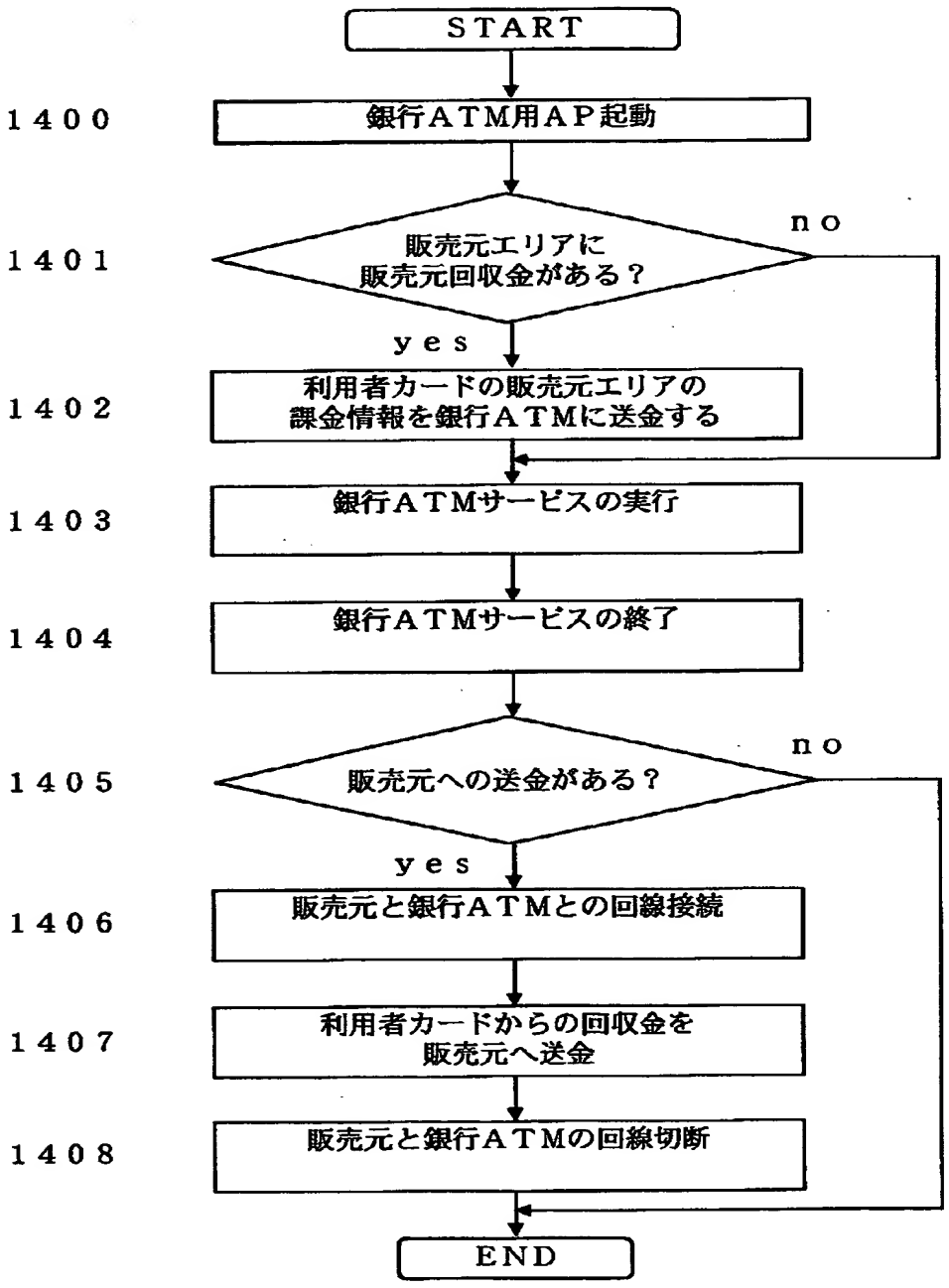
START
１４００
銀行ＡＴＭ用ＡＰ起動
１４０１
販売元エリアに
販売元回収金がある？
no
yes
１４０２
利用者カードの販売元エリアの
課金情報を銀行ＡＴＭに送金する
１４０３
銀行ＡＴＭサービスの実行
１４０４
銀行ＡＴＭサービスの終了
１４０５
販売元への送金がある？
no
yes
１４０６
販売元と銀行ＡＴＭとの回線接続
１４０７
利用者カードからの回収金を
販売元へ送金
１４０８
販売元と銀行ＡＴＭの回線切断
END

図１４

【図１５】

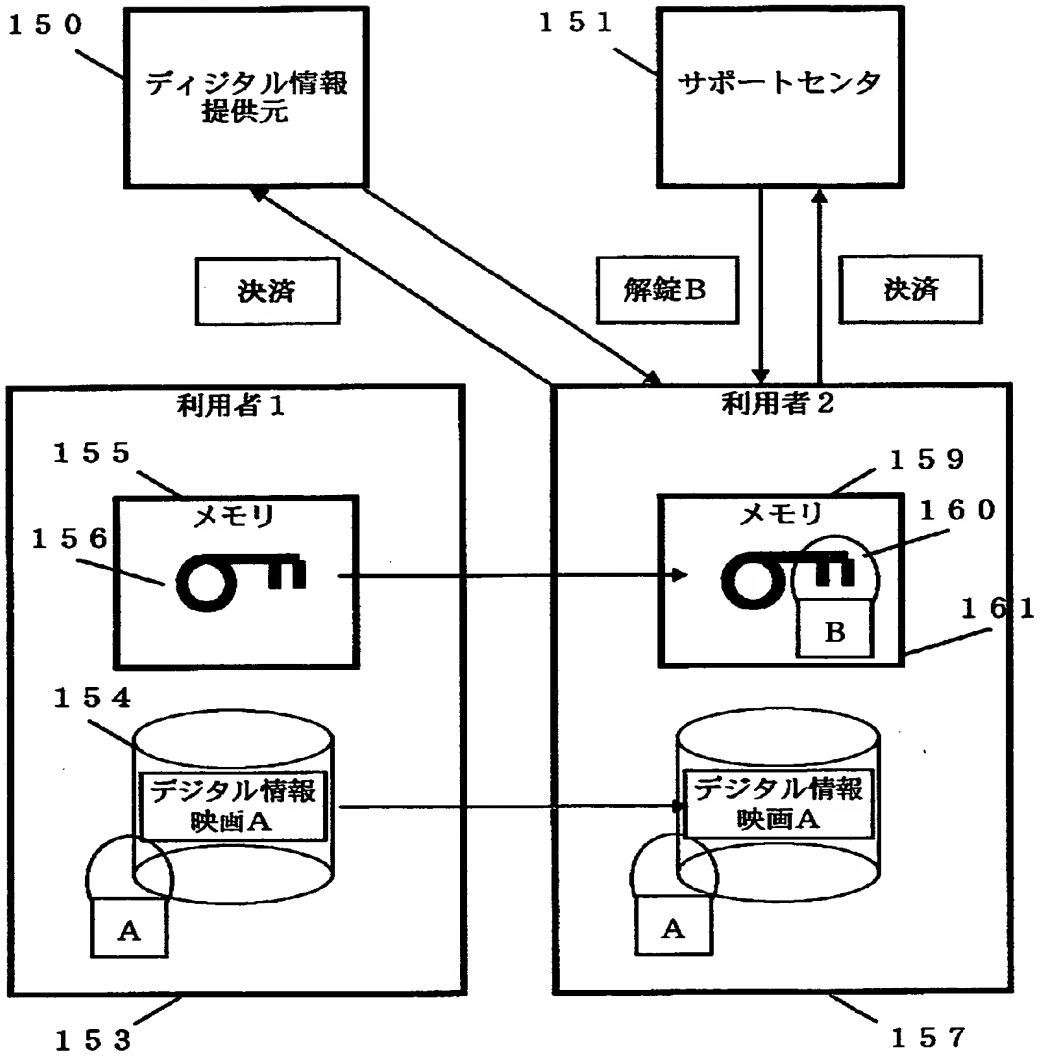
１５０
ディジタル情報提供元
１５１
サポートセンタ
決済
解錠B
決済
利用者１
利用者２
１５５
メモリ
１５６
１５９
メモリ
１６０
B
１６１
１５４
デジタル情報
映画A
A
デジタル情報
映画A
A
１５３
１５７

図１５

【図１６】

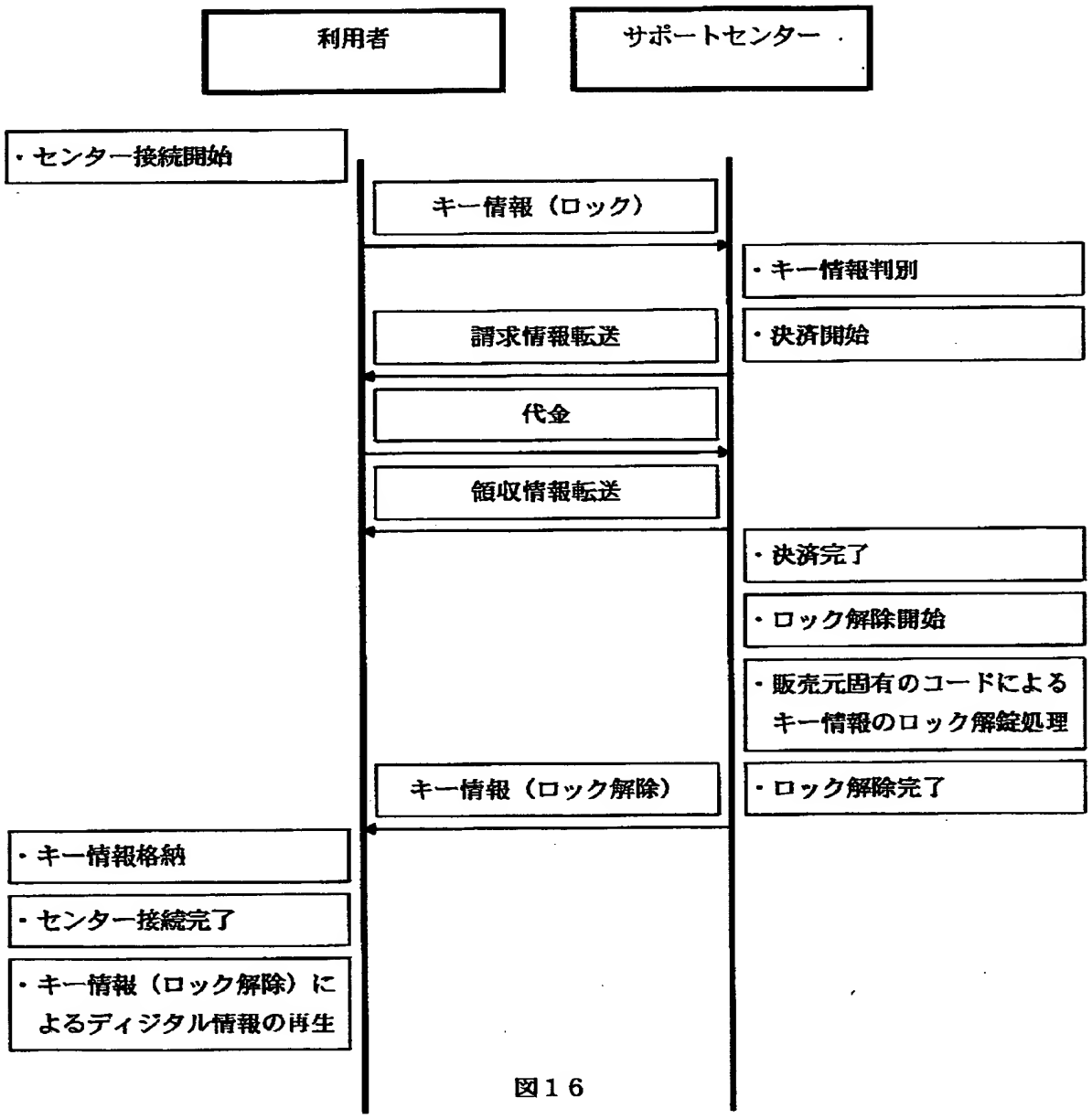

図１６

出証特２０００－３１０６２３９

【図１７】

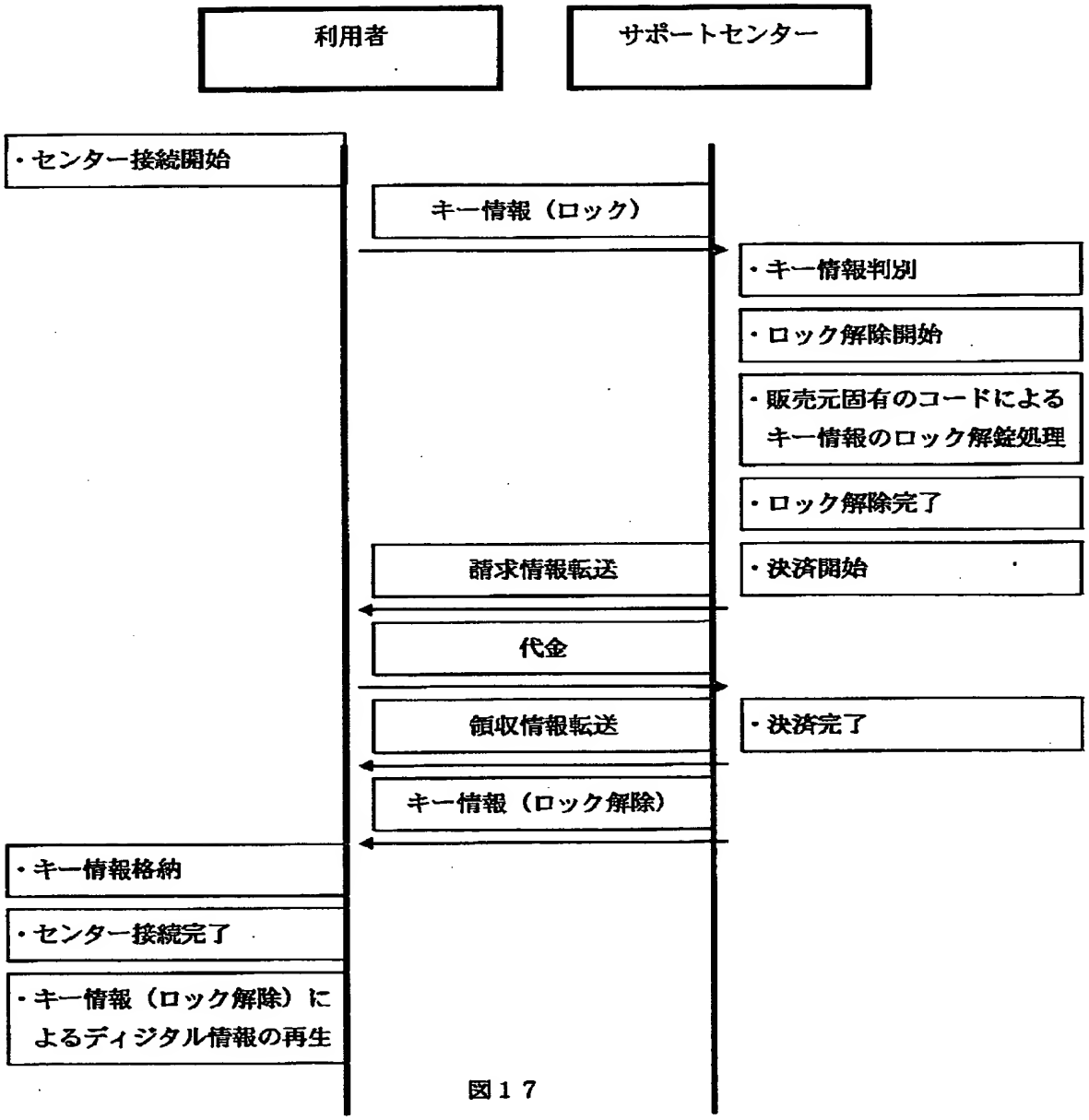

図１７

出証特２０００－３１０６２３９

【書類名】 要約書

【要約】

【課題】

ディジタル化された映像、音楽、著書などのディジタル情報に対する不正な複製を防止し、複製したディジタル情報の利用に伴う料金をディジタル情報の権利者へ確実に回収できる方法を提供する。

【解決手段】

ディジタル情報１５８の利用許可を行うキー情報１５６を複製する際には、ロックした状態で複製させ、キー情報１５６のロックを解除させる際には、販売元１５０へアクセスすることにより、ディジタル情報の利用料金を支払う。

【選択図】 図１５

出　願　人　履　歴　情　報

識別番号　　〔０００００５１０８〕

１．変更年月日　　１９９０年　８月３１日
［変更理由］　新規登録
住　所　東京都千代田区神田駿河台４丁目６番地
氏　名　株式会社日立製作所

出　願　人　履　歴　情　報

識別番号　　〔０００２３３１３６〕

１．変更年月日　　１９９１年　４月２４日
［変更理由］　名称変更
住　所　神奈川県横浜市戸塚区吉田町２９２番地
氏　名　株式会社日立画像情報システム